Zeszyty Naukowe AON nr 2(99) 2015
ISSN 2299-6753

płk dr Artur DĘBCZAK
Oddział Rozwoju Koncepcji
Centrum Doktryn i Szkolenia SZ

ppłk Cezary PAWLAK
Oddział Rozwoju Koncepcji
Centrum Doktryn i Szkolenia SZ

ANALITYCZNY MODEL OCENY HYBRYDOWOŚCI WSPÓŁCZESNYCH KONFLIKTÓW

kmdr por. Jarosław KEPLIN
Oddział Rozwoju Koncepcji
Centrum Doktryn i Szkolenia SZ

Streszczenie

Celem powyższego opracowania jest wyjaśnienie istoty działań hybrydowych, określenie ich przebiegu w poszczególnych fazach oraz zdefiniowanie i przedstawienie propozycji narzędzia (modelu analitycznego).

W opracowaniu scharakteryzowano hybrydowość współczesnych konfliktów oraz pojęcia zidentyfikowane podczas prac nad narodową Koncepcją udziału sił zbrojnych w przeciwdziałaniu zagrożeniom hybrydowym, realizowaną przez Centrum Doktryn i Szkolenia Sił Zbrojnych w ścisłej współpracy z grupą ekspertów dziedzinowych. Przedstawiono opracowaną propozycję modelu analitycznego opisującego przebieg możliwych zagrożeń we wszystkich rozpatrywanych obszarach, tj. politycznym, ekonomicznym, społecznym, militarnym, infrastruktury i informacyjnym (PEMSII).

Słowa kluczowe: bezpieczeństwo, hybrydowość, działania hybrydowe, strategia, zagrożenia, analityczny model działań hybrydowych

Wstęp

Metody stosowane podczas wojen XXI wieku wzbudzają szereg refleksji wśród licznych ekspertów na temat przyszłych środków i sposobów zapewniających bezpieczeństwo wewnętrzne i zewnętrzne państwa oraz stabilność regionu.

Kompleksowy charakter współczesnych konfliktów rozumiany jest jako szeroko pojęta *hybrydyzacja* i stanowi wyzwanie dla jej zrozumienia, a zarazem opracowania nowych rozwiązań do przeciwdziałania. Powinny one uwzględniać aktualne środowisko bezpieczeństwa, w tym jego asymetrię, podziały kulturowe i skutki uboczne globalizacji, gdyż stały się one obecnie jednym z głównych wyzwań dla zapewnienia bezpieczeństwa współczesnego świata.

Celem niniejszego artykułu jest wyjaśnienie istoty działań hybrydowych, ich zdefiniowanie oraz przedstawienie propozycji narzędzia do określenia przebiegu działań w poszczególnych fazach.

W części pierwszej opracowania scharakteryzowano hybrydowość współczesnych konfliktów oraz pojęcia zidentyfikowane podczas prac nad narodową koncepcją[1] realizowaną przez Centrum Doktryn i Szkolenia Sił Zbrojnych (CDiS SZ).

[1] Prace nad koncepcją realizowane są przez zespół projektowy CDiS SZ w ścisłej współpracy z grupą ekspertów dziedzinowych krajowych i zagranicznych. Prace te rozwijane są także w ramach Wielonarodowej Kampanii Rozwoju Zdolności (Multinational Capability Development Campaign – MCDC). Zakres pojęciowy w zakresie definicji i faz działań

W części drugiej, bazując na przyjętej terminologii oraz opisie faz, przedstawiono propozycję modelu analitycznego opisującego przebieg możliwych zagrożeń we wszystkich rozpatrywanych obszarach: politycznym, ekonomicznym, społecznym, militarnym, infrastruktury i informacyjnym (PEMSII)[2].

Działania hybrydowe – istota i terminologia

Współczesne konflikty zbrojne zarówno o charakterze regionalnym, jak i szerszym zasięgu, cechuje kompleksowość wykorzystania wszelkich możliwych środków. Wstępne analizy wskazują na zależności względem faz realizacji planu oraz przyjętych przez agresora celów polityczno-strategicznych. Ich kompleksowy charakter rozumiany jest jako szeroko pojęta hybrydyzacja i stanowi wyzwanie dla jej zrozumienia, a zarazem opracowania nowych rozwiązań w celu przeciwdziałania im.

Od kilku lat obserwuje się narastające wzajemne przenikanie i łączenie technik wojny regularnej i nieregularnej. Dodatkowo powszechnym zjawiskiem w polityce stało się uzależnianie ekonomiczno-gospodarcze przez potencjalnego agresora. Ponadto widoczne jest szerokie spektrum oddziaływania na społeczeństwa, grupy narodowe, etniczne czy religijne poprzez środki informacyjne i zabiegi dyplomatyczne. Doświadczenia wskazują, że rozwiązania te powinny uwzględniać m.in. obecne środowisko bezpieczeństwa, w tym jego asymetrię, podziały kulturowe i skutki uboczne globalizacji. Wynika to z faktu, że stały się one jednym z głównych wyzwań dla zapewnienia bezpieczeństwa współczesnego świata. Różnorodność środowiska bezpieczeństwa, a przede wszystkim skala wykorzystywanych środków, jest obecnie tematem licznych analiz i opracowań.

Można wnioskować, że kompleksowość działań oraz trudność ich wykrycia są efektem globalizacji, która może destrukcyjnie wpłynąć na narodowe sektory ekonomiczno-gospodarcze, pozwalając jednocześnie ukryć działania agresora, np. przez fikcyjne organizacje pozarządowe, firmy i korporacje.

Ponadto powszechny dostęp do informacji oraz manipulacja nią mają istotny wpływ na populacje, grupy mniejszości narodowych, etnicznych oraz religijnych, kreując tym samym panujące w nich nastroje. Zjawisko to powszechnie zaczęto nazywać *działaniami hybrydowymi* lub *wojną hybrydową*.

Etymologia terminu *hybrydowość* prowadzi do łacińskiego słowa *hybryda*, oznaczającego *mieszańca*, osobnika powstałego ze skrzyżowania dwóch genetycznie różnych osobników, należących do różnych gatunków odmian czy ras[3].

Jedną z pierwszych osób popularyzujących termin *wojna hybrydowa* był Frank G. Hoffman[4]. Według niego, wojna hybrydowa cechuje się *zbieżnością* [...] *fizyczną i psychologiczną, kinetyczną i niekinetyczną, bojowników i cywilów* [...] *sił zbrojnych i społeczności, państw i aktorów niepaństwowych, a także zdolności bojowych, w które są wyposażone*[5].

Termin *wojna hybrydowa* zawęża pojęcie hybrydowości i utożsamiane jest z siłami zbrojnymi, które stanowią de facto minimalną część w całym spektrum działań podjętych przez potencjalnego agresora. Ponadto należy zauważyć, że powszechnie używany w anglojęzycznych opracowaniach termin *hybrid warfare* jest błędnie interpretowany jako wojna hybrydowa. Hybrydowość niesie za sobą złożoność i wielopłaszczyznowość działań, dlatego należy wziąć pod uwagę liczne, często krytyczne uwagi dotyczące terminu *wojna hybrydowa*, w tym aspekty prawne bezpośrednio z nim związane, takie jak brak wypowiedzenia wojny oraz wprowadzenia stanu wyjątkowego lub wojennego.

Zrozumienie charakteru tych działań oraz dokonanie zmian w postrzeganiu współczesnych konfliktów wymusza dostosowanie istniejących i wypracowanie nowych dokumentów normujących funkcjonowanie wszystkich resortów państwa odpowiedzialnych za jego bezpieczeństwo.

hybrydowych uzgodniono w ramach prac grupy roboczej ds. rozwoju *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym* w dniu 16 września 2015 r. w Bydgoszczy.

[2] Metoda PEMSII zwana generalną segmentacją otoczenia. Dzieli otoczenie na: Polityczne, Ekonomiczne, Militarne, Społeczne, Infrastruktury, Informacyjne.

[3] *Słownik wyrazów obcych PWN*, Warszawa 1980, s. 290.

[4] Emerytowany ppłk marines, pracownik naukowy Instytutu Studiów Strategicznych Narodowego Uniwersytetu Obrony USA. Międzynarodowy Instytut Badań Politycznych (FPRI) www.fpri.org/taxonomy/tem/413/0.

[5] A. Gruszczak, *Hybrydowość Współczesnych Wojen – analiza krytyczna*. Artur Gruszczak www. bbn.gov, s.13. za Frank. G. Hoffman, *Hybrid Warfare and Challenges*, Joint Force Quarterly, 2009. Nr 52, s. 34.

Rozwiązania te mają przygotować struktury państwa do nowych wyzwań, w tym identyfikacji zagrożeń[6] i szacowania ryzyka[7]. Istnieje pilna potrzeba znalezienia nowych rozwiązań w zakresie zapewniania i utrzymywania bezpieczeństwa państwa oraz dostosowania strategii prowadzenia działań z użyciem sektora militarnego i pozamilitarnego, a przede wszystkim sposobów wykrywania symptomów zagrożeń i przeciwdziałania ich rozwojowi.

Biorąc pod uwagę szerokie spektrum, charakter i skalę działań oraz fakt, że celowo są ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się jednoznacznie zidentyfikować progu regularnej wojny, należy stosować w opracowaniach termin *działania hybrydowe* zamiast *wojna hybrydowa*.

Działania hybrydowe oddziałują na wszystkie lub wybrane obszary PEMSII z niejednolitą intensywnością oraz w różnym przedziale czasu, często w granicach obowiązującego prawa, zwłaszcza w początkowej fazie. Ich wzajemne relacje, przenikanie do kolejnych obszarów oraz powodowanie eskalacji zagrożeń wpisują się jako zespół przyczynowo-skutkowy w definicje ww. działań. W celu określenia możliwości wystąpienia działań hybrydowych należy scharakteryzować i skategoryzować obszary PEMSII pod względem ewentualnych zagrożeń z uwzględnieniem ich wagi, przyszłych trendów oraz występujących symptomów.

Należy zaznaczyć, że przede wszystkim działania hybrydowe muszą spełniać określone warunki dla powodzenia realizacji zakładanych celów długoterminowych. Oznacza to, że w każdym lub w kilku wybranych obszarach dane zagrożenia powinny osiągnąć tzw. punkty przełamania[8] w celu powodzenia realizacji planu, aby utrudnić lub uniemożliwić przeciwdziałanie. Większość tych przedsięwzięć realizowanych jest w pierwszej fazie jako działania skryte, wykorzystujące dane otoczenie, uwzględniające własny potencjał oraz zmiany i trendy w środowisku bezpieczeństwa. Dotychczasowe doświadczenia oraz te z przeszłości wskazują, iż obszar społeczny oraz ekonomiczny stanowią największe i najpoważniejsze zagrożenie. Przykładem są działania prowadzone na wschodzie Ukrainy oraz przez tzw. Państwo Islamskie.

Ujednolicenie glosariusza terminologii[9] w obszarze działań hybrydowych pozwoliło na opracowanie faz działań hybrydowych oraz modelu działań hybrydowych.

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 W. Gierasimowa[10], który przedstawił swój model[11] 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.

Na uwagę zasługuje także opracowanie fińskie[12]. Ujęto w nim sześć faz takich działań:

- przygotowanie strategiczne,
- przygotowanie polityczne,
- przygotowanie operacyjne,
- eskalacja napięcia,

[6] Zagrożenia – wszelkie destrukcyjne oddziaływania na podmiot, egzemplifikujące się w postaci sytuacji kryzysowych, a nawet kryzysów. Patrz szerzej: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

[7] Ryzyko – prawdopodobieństwo wystąpienia niekorzystnego zdarzenia wraz z jego skutkami w określonym czasie. Ocena ryzyka na potrzeby zarządzania kryzysowego. Rządowe Centrum Bezpieczeństwa. Warszawa 2013, s. 13.

[8] Dla niniejszego opracowania przyjęto, że w układzie współrzędnych kartezjańskich punktem przełamania, jest punkt na wykresie obrazujący moment identyfikacji zagrożenia, gdzie należy podjąć wysiłki do zniwelowania skutków oddziaływania agresora. Zmienna ta na wykresie, charakteryzuje się zmianą jej wypukłości. Patrz Rys. nr 3. Przykładowy wynik analitycznego modelu zagrożeń hybrydowych.

[9] Terminologia została zawarta w załączniku nr 1.

[10] Generał Walerij Gierasimow – Szef Sztabu Generalnego Federacji Rosyjskiej.

[11] Przekład z: Валерий Герасимов, Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

[12] Andras Racz, Russia's Hybrid War in Ukraine. Fiński Instytut Stosunków Międzynarodowych Raport 43 z 2015, s. 59–63.

– obalenie władzy centralnej w regionie docelowym,

– ustanowienie alternatywnej władzy.

Dla porównania w opracowaniu łotewskiej[13] 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.

Brak jednolitych opracowań w tym zakresie w NATO oraz państwach UE spowodowały konieczność podjęcia prac narodowych[14].

Dla pełnego zrozumienia badanej kwestii zespół autorski poddał analizie konflikty z elementami hybrydowymi, takie jak: w Somalii, w Libanie, na wschodzie Ukrainy oraz działania Państwa Islamskiego. W wyniku tych prac ujednolicono wszystkie występujące przypadki jako uniwersalne fazy przebiegu działań hybrydowych.

Wyróżniono następujące fazy działań hybrydowych (tab. nr 1). Szczegółowy opis faz przedstawiono w zał. nr 2:

– przygotowania;

– destabilizacji;

– działań militarnych;

– rozstrzygnięcia.

Tabela 1

Poglądowy schemat faz działań hybrydowych

FAZA I PRZYGOTOWANIA		FAZA II DESTABILIZACJI	FAZA III DZIAŁANIA MILITARNE	FAZA IV ROZSTRZYGNIĘCIE
CZĘŚĆ SKRYTA	CZĘŚĆ JAWNA			

Opracowanie własne.

Działania w fazie przygotowania można podzielić na dwie części: skrytą i jawną. Działania w części skrytej mają charakter niejawny. Charakteryzują się m.in. tym, że wykorzystywane są różnego rodzaju sposoby nacisku i wpływu kierowane przez korporacje, organizacje pozarządowe i religijne. Cechą szczególną tej fazy jest to, że potencjalne państwo, które jest celem ataku, nie jest świadome, że są prowadzone przeciwko niemu skoordynowane działania. Ich znaczenie jest kluczowe dla przygotowania i prowadzenia dalszych działań przez agresora. Działania te przechodzą w część jawną wtedy, kiedy państwo będące celem ataku **zauważa** działania wymierzone przeciwko niemu. W tej części fazy można dostrzec tworzenie atmosfery nieuchronności krachu finansowego, bezradność organów rządzących, słabość resortów siłowych oraz możliwość wystąpienia konfliktu zbrojnego przy zachowaniu dotychczasowej polityki zarówno na arenie dyplomatycznej, jak i gospodarczej. Następuje psychologiczne i ideologiczne rozbudzanie separatyzmów i dążeń ideologicznych lub religijnych.

Efektywna realizacja fazy przygotowania gwarantuje przejście do kolejnej – fazy destabilizacji. Charakteryzuje się ona m.in. zakłóceniem działania centralnych i lokalnych ośrodków władzy, struktur siłowych, przedstawicieli mediów i biznesu przy wykorzystaniu metod i narzędzi powszechnie stosowanych (politycznych, ekonomicznych, gospodarczych i społecznych, itp.), jak i zaawansowanych technologicznie (np. cyberatak). W tej fazie wyszczególnić można szeroko zakrojone działania informacyjne – opcjonalnie dezinformacyjne (na wszystkich poziomach: od komunikacji strategicznej po przekazy lokalne) za pomocą wszelkich dostępnych środków przekazu

[13] Janis Berzins, Rassia's New Generation Warfare in Ukraine. Implikations for Latvian Defense Policy National Defence Academy of Latvia. Policy Paper nr 2 z 2014, s. 6. Za Techikinov i Bogdanov 2013, s. 15–22.

[14] Zadanie opracowania *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym*, zlecone przez Szefa Sztabu Generalnego WP.

informacji na obszarze ewentualnego konfliktu oraz w jego otoczeniu międzynarodowym w celu osiągnięcia pożądanej reakcji. Jeżeli celem głównym agresora będzie jedynie destabilizacja pewnych obszarów danego kraju, to działania te mogą się zakończyć. W przypadku, gdy cele agresora nie są całkowicie osiągnięte, może on przejść do kolejnej fazy, tj. działań militarnych.

Na tym etapie zauważyć można m.in. tworzenie lokalnych oddziałów separatystów złożonych np. z mniejszości narodowych lub religijnych działających przy wsparciu przywódców duchowych, organizacji terrorystycznych, sił zbrojnych oraz służb specjalnych agresora. Ich głównym zadaniem jest podsycanie napięcia, potwierdzenie bezradności władz oraz zablokowanie możliwości prowadzenia akcji przez resorty, siłowe np. policję, armię atakowanego kraju i w skoordynowany sposób przejęcie kontroli nad kluczowymi obiektami i obszarami mającymi wpływ na powodzenie operacji. Do obiektów posiadających szczególne znaczenie można zaliczyć m.in. przejścia graniczne, stacje przekaźnikowe mediów, kluczową infrastrukturę taką jak główne skrzyżowania dróg, mosty oraz węzły kolejowe i lotniska. Należy podkreślić, że w tej fazie działania militarne wspierane są przez skoordynowane i szczegółowo zaplanowane działania dyplomatyczne oraz informacyjne.

Ostatnią zdefiniowaną fazą jest rozstrzygnięcie. Charakteryzuje się ona ustanowieniem władz centralnych i lokalnych zależnych od agresora. Rozstrzygnięciem jest przede wszystkim akceptacja wymuszonej sytuacji politycznej. Przy niepowodzeniu zakładanych celów działań hybrydowych, po fazie działań militarnych może dojść do otwartego regularnego konfliktu zbrojnego. Jednakże w tym przypadku **nie są to** działania hybrydowe.

Analityczny model działań hybrydowych

Zagrożenia we współczesnym świecie charakteryzują się różnorodnością i złożonością ich występowania. Warto podkreślić, że bezpieczeństwo państwa[15] nie jest jedynie stanem, ale przede wszystkim dynamicznym procesem, na który mają wpływ różnorodne determinanty[16]. Powoduje to trudności w dokonaniu właściwej oceny zagrożenia. Złożoność jego występowania w poszczególnych obszarach znacznie komplikuje możliwość znalezienia właściwej metodyki, niezbędnej do określenia faktycznego wpływu na zagrożenia[17].

Zasadne jest wykorzystanie metody modelowania[18]. Tworząc modele i konfrontując je z rzeczywistością m.in. poprzez obserwację, sprawdza się, jakie prawa rządzą zachodzącymi zjawiskami. Zrozumienie powyższego stanowi inherentny czynnik pozwalający przewidzieć przebieg zjawisk w przyszłości[19]. Dotyczy to także problematyki bezpieczeństwa państwa. Jak zauważa Anna Antczak-Barzan[20] *brak umiejętności identyfikacji potencjalnych zagrożeń w ujęciu długofalowym na podstawie rozwijających się trendów wewnętrznych i zewnętrznych (w bliższym i dalszym otoczeniu państwa) może prowadzić do katastrofy. Polityka krótkowzroczności oraz dbania o partykularne prywatne interesy oraz walki pomiędzy poszczególnymi frakcjami politycznymi już nieraz doprowadziły nasze państwo do klęski*[21].

Powyższe ustalenia i wnioski są podstawą do stwierdzenia, że zidentyfikowane zagrożenia powinny być poddane systematycznej analizie i monitorowaniu. Obecnie opracowany analityczny model zagrożeń hybrydowych ma za zadanie pomóc zrozumieć symptomy i mechanizmy powstawania zagrożeń, a także umożliwić identyfikowanie nowych, które mogą w istotny sposób wpłynąć na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogą mieć istotne znaczenie dla bezpieczeństwa zarówno wewnętrznego, jak

[15] Bezpieczeństwo państwa – taki rzeczywisty stan stabilności wewnętrznej i suwerenności państwa, który odzwierciedla brak lub występowanie jakichkolwiek zagrożeń (w sensie zaspokojenia podstawowych potrzeb egzystencjonalnych i behawioralnych społeczeństwa oraz traktowania państwa jako suwerennego podmiotu w stosunkach międzynarodowych). *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydanie szóste, AON, Warszawa 2002, s. 19.

[16] Szerzej zob. A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 226.

[17] Zagrożenia – wszelkie destrukcyjne oddziaływania na podmiot, egzemplifikujące się w postaci sytuacji kryzysowych, a nawet kryzysów. Patrz szerzej: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

[18] Modelowanie matematyczne i badanie złożonych układów analitycznych. Maciej Rymanowski, Kraków 2007, s. 11.

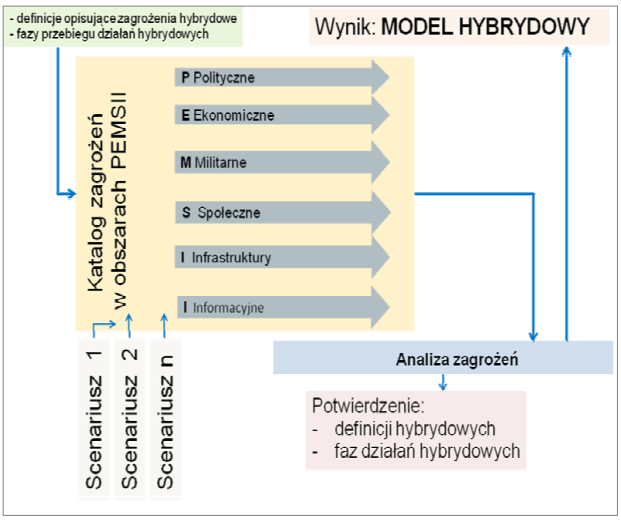
[19] Ibidem.

[20] Dr hab nauk społecznych w zakresie nauk o polityce (PAN).

[21] A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 238.

i zewnętrznego. Takie podejście powinno również przyczynić się do przygotowania narzędzi przeciwdziałania potencjalnym zagrożeniom.

Przygotowując analityczny model działań hybrydowych przyjęto określone założenia. Po pierwsze, prace prowadzi się w oparciu o metodykę zarządzania projektem PRINCE2[22]. Miało to na celu wykorzystanie efektywnych zasad zarządzania, które są niezbędne podczas realizacji projektu, w tym zapewnienia usystematyzowanego podejścia gwarantującego jego powodzenie. Niemniej należy pamiętać, iż metodyka ta dostarcza wiedzę na temat stosowanych technik, ale nie precyzuje szczegółowo jak z nich korzystać. Kolejne ustalenie to określenie danych wejściowych. Zaliczono do nich: katalogi zagrożeń w obszarach PEMSII, definicje z obszaru zagrożeń hybrydowych oraz fazy przebiegu działań hybrydowych. Na potrzeby opracowania analitycznego modelu założono także, że środowisko bezpieczeństwa będzie podzielone na obszary: polityczne, ekonomiczne, militarne, społeczne, infrastruktury oraz informacyjne. Zespół autorski w trakcie prowadzonych badań zdefiniował dla każdej z wymienionych domen osobny katalog zagrożeń wraz z ich charakterystyką. Ideę modelu przedstawia rys. 1:

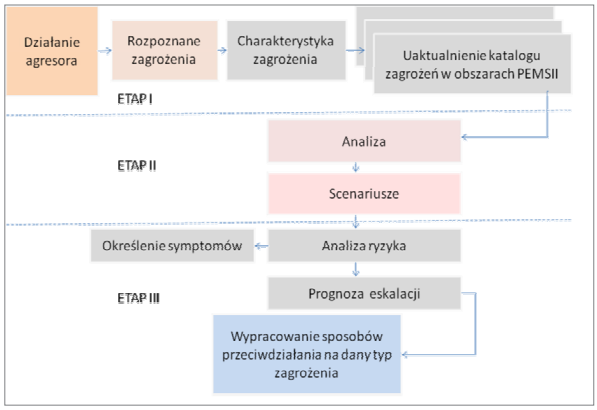


Opracowanie własne.

Rys. 1. Schemat ideowy analitycznego modelu zagrożeń hybrydowych

[22] PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009. Metodyka zarządzania projektami. Stosowana do sterowania i zarządzania projektami.

W trakcie opracowywania modelu hybrydowego przyjęto następującą metodologię procesu przetwarzania danych (rys. 2):



Opracowanie własne.

Rys. 2. Metodologia procesu analizy zagrożenia

W pierwszym etapie procesu, na podstawie zagrożeń wynikających z działania agresora, dokonuje się charakterystyki zagrożenia i umieszczenia go w katalogach. W drugim etapie wybiera się newralgiczne zagrożenie celem przeprowadzenia jego analizy oraz opracowania scenariuszy przypadków. Scenariusze te obejmują ogół czynności mających na celu zrozumienie czynników wywołujących te zagrożenia oraz symptomy ich powstania i zachodzące między nimi związki. W ramach tego etapu poszczególne zagrożenia bada się m.in. ze względu na:

– intencje: interes, potrzeby, politykę, wolę,

– możliwości: zdolności, metody, zasoby, ograniczenia,

– dane historyczne: przypisane incydenty, podejmowane próby, potwierdzone operacje, częstotliwość, efektywność tych działań,

– sygnały: nowe potwierdzone lub niepotwierdzone dowody.

Takie podejście daje możliwość oszacowania ryzyka wystąpienia zagrożeń. W założeniach przyjęto, że przy szacowaniu ryzyka istotne będą: zidentyfikowane zagrożenia z katalogu, prawdopodobieństwo zaistnienia, podatność obszarów PEMSII oraz ich wpływ i skutki na bezpieczeństwo państwa. Należy podkreślić, że oszacowanie wartości dwóch podstawowych parametrów składowych, tj. prawdopodobieństwa i skutków, jest kluczowe dla określania podatności na ryzyko. Poziom ryzka szacowany jest w oparciu o użycie dyskretnej skali stopniowania prawdopodobieństwa, która została przedstawiona poniżej (tab. 2).

Tabela 2

Dyskretna skala stopniowania prawdopodobieństwa

MAŁO PRAWDO-PODOBNE	Zagrożenia wcześniej niezidentyfikowane i nieudokumentowane, które mogą wystąpić tylko w wyjątkowych i sprzyjających okolicznościach. Przyjmują wartość 0–20%
RZADKIE	Zagrożenia udokumentowane, symptomy czy też inne okoliczności zagrożenia są mało znane. Przyjmują wartość 20–40%
MOŻLIWE	Zagrożenia udokumentowane, symptomy czy też mechanizm powstawania znany. Może zdarzyć się w określonym czasie w sprzyjających warunkach. Przyjmują wartość 40–60%
PRAWDO-PODOBNE	Zagrożenia znane i wcześniej spotykane. Jest prawdopodobne, że w przypadku sprzyjającego środowiska wystąpią w większości okoliczności. Przyjmują wartość 60–80%
BARDZO PRAWDO-PODOBNE	Zagrożenia doskonale znane i systematyczne. Panuje odpowiednie środowisko dla ich powstania. Oczekuje się, że zagrożenia te zdarzą się w większości okolicznościach. Przyjmują wartość 80–100%

Źródło: Opracowanie własne w oparciu o: *Ocenę ryzyka na potrzeby zarządzania kryzysowego*, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

Oszacowana wartość ryzyka na matrycy odzwierciedla zależność pomiędzy prawdopodobieństwem oraz skutkami[23]. Każdemu zidentyfikowanemu ryzyku odpowiada jedno określone pole (patrz tab. 3).

Tabela 3

Matryca ryzyka

MATRYCA RYZYKA						
PRAWDOPODOBIEŃSTWO	MAŁO PRAWDOPODOBNE	S	S	W	W	K
	RZADKIE	S	S	S	W	W
	MOŻLIWE	M	S	S	S	W
	PRAWDOPODOBNE	M	M	S	S	S
	BARDZO PRAWDOPODOBNE	N	M	M	S	S
		NIEISTOTNE	MAŁE	ŚREDNIE	DUŻE	EKSTREMALNE
SKUTKI						

N – Nieistotne M – Małe Ś – Średnie H – Wysokie E – Katastrofalne

Źródło: Opracowanie własne na podstawie: Field Manual No. 5–19 (100–14), Composite Risk Managemement, Department of the Army. Washington, DC, July 2006 oraz Oceny ryzyka na potrzeby zarządzania kryzysowego. Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

[23] Skutek – faktyczne konsekwencje jakiegoś działania. Na podstawie PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009, s. 27.

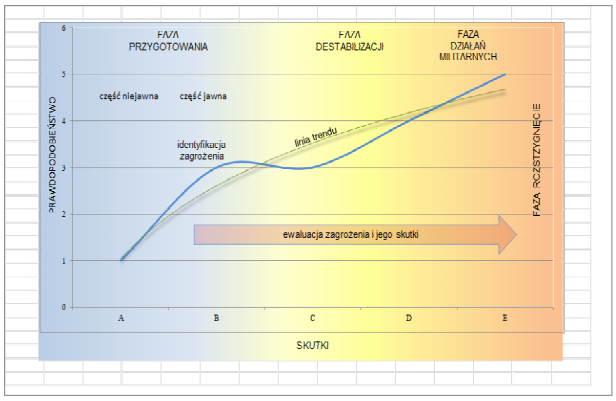
W dalszej kolejności, bazując na ocenach podatności na ryzyko dla wszystkich zidentyfikowanych zagrożeń, uzyskane dane umieszcza się w arkuszu klasyfikacyjnym, gdzie następuje ich grupowanie i wartościowanie w obszarach PEMSII wraz z opisem ich skutków. Zgodnie z przyjętą skalą (tab. 3) hierarchizuje się ryzyko od najbardziej do najmniej istotnego. W tym przypadku wyróżnić można dwa różne podejścia. Pierwsze z nich traktuje czynniki ryzyka, które posiadają najwyższe prawdopodobieństwo wystąpienia jako najistotniejsze, a drugie postrzega wpływ na obszary otoczenia jako najważniejszy.

Takie podejście umożliwia powiązanie ze sobą zagrożeń i dodatkowo ułatwia identyfikację szans[24] oraz określenie trendu. W konsekwencji może pomóc to w ich przeciwdziałaniu oraz wykryciu wcześniejszych symptomów, które w normalnej działalności mogłyby być niezauważone.

Zaprezentowany model pozwala na wyodrębnienie z istniejącej grupy wyzwań w środowisku bezpieczeństwa konkretnych szans i zagrożeń dla danego obszaru. Odzwierciedla on jednocześnie przebieg i rozwój zagrożenia z uwzględnieniem faz działań hybrydowych.

Poniższy rysunek (rys. 3) przedstawia poglądowy wynik wybranego zagrożenia, umiejscowionego w układzie współrzędnych, gdzie osi odciętych nadano wartości skutków, a na osi rzędnej zobrazowano prawdopodobieństwo wystąpienia danego typu zagrożenia. Na podstawie uzyskanych wyników wyraźnie widać działania podjęte przez agresora – określone przy pomocy krzywej oznaczonej kolorem niebieskim. Pełna identyfikacja zagrożenia następuje w chwili osiągania przez to zagrożenie punktu przełamania. Dodatkowo pozwala to obserwować ewaluację zagrożenia w poszczególnych fazach działań, przy braku podjęcia efektywnego przeciwdziałania. Ponadto umożliwia to wyznaczenie linii trendu. Na podkreślenie zasługuje fakt, że tak przeprowadzona analiza zagrożeń daje możliwość wypracowania strategii przeciwdziałania.

[24] Szanse – wszelkie okoliczności sprzyjające osiągnięciu interesu podmiotu. Patrz szerzej: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.



Opracowanie własne.

Rys. 3. Przykładowy wynik na podstawie analitycznego modelu zagrożeń hybrydowych, w jednym z obszarów PEMSII

W opracowaniach Anny Antczak-Barzan można dostrzec podobny sposób metodologii przy określaniu szans i zagrożeń w kontekście badania środowiska bezpieczeństwa Polski. Zauważa ona, że subiektywny dobór zmiennych nie pozwala na pełne zobrazowanie tego, co kryje się za poszczególnymi szansami czy zagrożeniami.

Podkreśla ona, że w pierwszej kolejności istnieje konieczność szerszego spojrzenia na dane zagrożenie, aniżeli wyciągania bezpośrednich wniosków. Według autorki *ostateczny wynik uzależniony jest od liczby szans i zagrożeń jakie można zidentyfikować w obszarze z każdego wyzwań, a tych może być bardzo wiele.* Dodatkowo wskazuje ona, że wyzwania same w sobie sygnalizują więcej zagrożeń niż szans, a część z nich jest realna, gdyż *albo już [one] występują, albo jeśli obecny kurs zostanie utrzymany, istnieje niemal pewność, że wystąpią [one] w najbliższej przyszłości, a wiele szans jedynie potencjalnych – zaistnieją w sytuacji, gdy spełnione zostaną liczne warunki*[25].

Celowość przyjętych rozwiązań w polskim modelu analitycznym oraz opracowanych faz działań hybrydowych potwierdziły opinie ekspertów krajowych i zagranicznych w ramach prowadzonych prac grupy roboczej w Multinational Capability Development Campaign (MCDC).

[25] Na podstawie: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 228.

Podsumowanie

Hybrydowość współczesnych konfliktów należy postrzegać jako konglomerat wszystkich działań podjętych przez potencjalnego agresora lub agresorów w obszarach PEMSII. Przeciwdziałanie tym zjawiskom nie jest wg. utartych schematów domeną samych sił zbrojnych czy układu pozamilitarnego, których faktyczne użycie następuje w trzeciej fazie działań hybrydowych. Opracowane definicje i fazy działań hybrydowych pozwoliły na usystematyzowanie zachodzących zjawisk. Dodatkowo narzędzie, jakim jest analityczny model działań hybrydowych, pozwala na identyfikację zagrożeń oraz umożliwia wyznaczenie ryzyka i ich ewentualnej eskalacji. Działanie takie pozwoli na opracowanie strategii przeciwdziałania zagrożeniom. Wymaga to jednak wysiłku międzyresortowego w celu osiągnięcia synergii, uaktualniania katalogów zagrożeń z uwzględnieniem aktualnej sytuacji międzynarodowej, stanu zewnętrznego i wewnętrznego państwa oraz trendów ich rozwoju w strategii długoterminowej. Brak umiejętności identyfikacji potencjalnych zagrożeń w ujęciu długofalowym może prowadzić w konsekwencji do nieodwracalnych skutków.

Bibliografia

Antczak-Barzan A., *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014.

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.

Валерий Герасимов. Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

Gruszczak A., *Hybrydowość Współczesnych Wojen – analiza krytyczna*. www. bbn.gov.

Hoffman F.G., *Hybrid Warfare and Challenges*, Joint Force Quarterly, JFQ Wyd. 51 2009.

Koziej S. i Brzozowski A., *Nauki o bezpieczeństwie: potrzeby i oczekiwania praktyki bezpieczeństwa narodowego. Tożsamość nauk o bezpieczeństwie*, Instytut Nauk Politycznych Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski, Wydawnictwo Adam Marszałek.

Materiały z prac grupy roboczej w ramach Wielonarodowej kampanii Rozwoju Zdolności (*Multinational Capability Development Campaign* – MCDC).

Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009.

Racz A., *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs, FIIA Report, Helsinki 2015.

Rymanowski M., *Modelowanie matematyczne i badanie złożonych układów analitycznych*, Kraków 2007.

Słownik wyrazów obcych PWN, Warszawa 1980. Por. Webster's New World Dictionary. wyd. 2. Prentice Hall Press. Nowy Jork 1986.

Sokala W., Zapała B., *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, Wydawnictwo BBN.

Zdrodowski B., *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014.

Załącznik 1

TERMINOLOGIA Z OBSZARU DZIAŁAŃ HYBRYDOWYCH

Załącznik ten przedstawia wybrane definicje wg terminologii opracowanej przez grupę ekspercką w ramach rozwoju *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym.*

Strategia działań hybrydowych

zapewnia osiągnięcie celów z wykorzystaniem dostępnego potencjału przy uwzględnieniu zmian i trendów w otoczeniu. W zależności od fazy planu jej wdrażania, realizowana jest w sposób skryty lub jawny przy wykorzystaniu instrumentów niemilitarnych i militarnych.

Działania hybrydowe

działania mające na celu osiągnięcie celów politycznych i strategicznych z możliwością utrzymania dotychczasowych stosunków gospodarczych i/lub dyplomatycznych. Działania te prowadzone są przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany oraz łączą różne środki wywierania nacisku i uzależniania od potencjalnego agresora. Mogą być one prowadzone w środowisku politycznym, ekonomicznym, militarnym i społecznym, w tym mniejszości narodowych, etnicznych i religijnych.

Model działań hybrydowych

przyjęty sposób działania ograniczony zdolnościami i wolą potencjalnego agresora, występujący we wszystkich lub wybranych obszarach: politycznym, ekonomicznym, militarnym, społecznym, informacyjnym i infrastruktury.

Załącznik 2

FAZY DZIAŁAŃ HYBRYDOWYCH

Załącznik ten przedstawia fazy działań hybrydowych zdefiniowane przez grupę ekspercką w ramach rozwoju *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym.*

FAZA I – Przygotowanie

1a część skryta

Działania w tej fazie mają charakter niejawny, poprzez wspieranie oraz wykorzystanie różnego typu grup nacisku i wpływu. Ich znaczenie jest kluczowe dla przygotowania i prowadzenia dalszych działań

1b część jawna

Ma miejsce w przypadku ujawnienia symptomów działań hybrydowych. Prowadzący je tworzy atmosferę sprzyjającą kontynuowaniu osiągania celów, zarówno w wymiarze wewnętrznym, jak i międzynarodowym.

FAZA II Destabilizacja

Zakłócenie funkcjonowania ośrodków władzy, struktur bezpieczeństwa, z wykorzystaniem środowiska informacyjnego we wszystkich lub wybranych obszarach, między innymi politycznym, ekonomicznym i społecznym. Faza ta może być celem samym w sobie lub obejmować osiąganie innych celów pośrednich.

FAZA III Działania militarne

Wykorzystywanie i wspieranie grup paramilitarnych i/lub regularnych sił zbrojnych. Aktywności tej towarzysza działania niemilitarne, w tym także dyplomatyczne oraz informacyjne.

FAZA IV Rozstrzygniecie

Akceptacja powstałej sytuacji politycznej.

ANALYTICAL MODEL AS A TOOL USED IN DESCRIBING CONTEMPORARY HYBRID CONFLICTS

Abstract

The aim of the article is to give a vivid insight into the essence of hybrid activity, to define the course of it in individual phases and to present the proposed tool, namely the analytical model. The article analyses the contemporary hybrid warfare and the terms formulated based on the works devoted to create the national Concept of Armed Forces Contribution in Countering Hybrid Warfare implemented by the Doctrine and Training Centre of PAF, in close cooperation with the group of subject matter experts. The article specifies the proposed analytical model concerning the course of possible threats in all PEMSII model fields, namely political, economic, social, military, information and infrastructure.

Key words: security, hybridity, hybrid activity/warfare, strategy, threats, hybrid warfare analytical model

Introduction

Methods used during the wars of the 21st century cause doubts among experts, especially when it comes to future means and ways that provide the internal and external security of a country and the stability of a region.

The complex manner of contemporary conflicts can be understood as broadly defined hybridity and it represents a real challenge, not only for understanding its role, but also for looking for new solutions in order to counter it. These solutions should provide for current environmental security, including its asymmetry, cultural splits and the side effects of globalisation, for they have become one of the main current challenges concerning the provision of contemporary world security.

The aim of the article is to explain the essence of hybrid warfare, to define it and to present the proposed tool used to define the course of activity in certain phases.

The first part of the article covers the hybridity of contemporary conflicts and it explains the terms highlighted based on the works devoted to create the national concept implemented by the Doctrine and Training Centre of PAF.

Based on the agreed terminology and the phase description, the second part of the article presents the recommended analytical model that describes the course of possible threats in all PEMSII areas, which are political, economic, social, military, infrastructure and informational.

Hybrid warfare – the essence and terminology

Contemporary armed conflicts of a regional and broader scope are characterised by the complexity of use of all the possible means. The preliminary analyses show the dependencies concerning plan implementation phases and the political and strategic aims represented by the aggressor. Their complex manner is very often understood as broadly defined hybridisation and reflects the challenge, not only of becoming familiar with the ideas themselves, but also to come up with new solutions in order to counter them.

In the last few years, there has been a growing tendency to join and combine regular and irregular war techniques. Additionally, economic subservience by the potential aggressor has become a very common phenomenon in the political sphere. What is more, the use of informational means and diplomatic measures as part of a very broad spectrum of influence on societies, national ethnic and religious groups has become more visible than before. The recent past has shown that these solutions should include, among others, the current environmental security (with its asymmetry, cultural splits and the side effects of globalisation). This is connected to the fact they have become one of the main challenges for providing contemporary world security. The diversity of environmental security and, above all, the scale of means used is the background for heated debate nowadays which can be seen in the numerous analyses and research papers.

It can be assumed that the complexity of all the above mentioned activities and the difficulty in identifying them are the effect of globalisation, which can have a disruptive influence on national economic sectors keeping the aggressor's activity hidden by, for instance, creating fictional non-governmental organisations, companies and corporations at the same time.

What is more, the universal access to information and the activity focused on manipulating it significantly influence the populations, national and ethnic and religious minorities creating a certain atmosphere within them. This phenomenon has started to be called hybrid warfare or hybrid warfare.

The word 'hybridity' derives from Latin, meaning hybrid – which stands for the offspring of two creatures of different 'half-blood species'.

One of the first people to bring the term 'hybrid warfare' into general use was Frank G. Hoffman. According to him, hybrid warfare is defined by the "convergence of the physical and psychological, the kinetic and non-kinetic, and combatants and noncombatants, convergence of military force and the interagency community, of states and non-state actors, and of the capabilities they are armed with.

The term 'hybrid warfare' narrows down the idea of hybridity and is often equated with armed forces, which, in fact, are only a marginal part of the whole spectrum of the potential aggressor's activity. Moreover, it has to be stated that the term *hybrid warfare*, which is broadly used in documents in English, is very often interpreted incorrectly as a hybrid war. Hybridity generates complexity and multidimensionality of activity, so one should take into account numerous, often critical remarks concerning the term *hybrid warfare*, including legal aspects directly connected with it, which are: the lack of declaring war or state of emergency/war.

The awareness of the manner of such activity and introduction of changes in perceiving of contemporary conflicts impose the adapting of the actual and providing new documents regulating/ standardising the functioning all states responsible for their security. Such solutions are there to prepare the state's structure for new challenges, including identification of threats and risk calculation. The need arose to find new solutions concerning providing and maintaining state security and adjusting the strategy for carrying out activities with the use of the military and non-military sector, above all with the measures focused on identifying the symptoms of threats and countering their progression.

Taking into account the broad spectrum, the scale of activity and the fact that they are intentionally constricted and kept on the level below the possible threshold of regular war by the aggressor, the term 'hybrid warfare instead of 'hybrid war' is recommended for use in latter documents.

Hybrid warfare activity has an impact on practically all or selected PEMSII areas with an uneven intensity and in a different period of time, often balancing upon the boundaries of existing law, especially at the initial phase. Their mutual relations, interpenetration into other areas and causing escalation of threats on the basis of cause and effect dependency comply with the definitions of the above mentioned activity. In order to precisiely define the possibility of the occurrence of hybrid warfare, one needs to highlight and categorize PEMSII areas with regard to potential threats, bearing in mind their importance, future trends and actual symptoms.

It should be mentioned that hybrid warfare needs to fulfill certain requirements when it comes to the successful implementation of deemed long-term goals. This means that in every, or in a few selected areas, certain threats should reach so called "breaking points" in order to successfully fulfill the plan/ schedule and to hinder or indispose countering them. Most of these actions take place in the first phase, as covert activity making use of a certain environment and taking into account their own potential and changes in the environmental security. It can be stated that, so far, the social and economic areas are the biggest and the most serious threats. Activities on the territory of Ukraine and Islamic Countries may provide examples.

The unification of the glossary concerning hybrid warfare allowed hybrid warfare phases and the hybrid warfare model to be provided for.

The phases of hybrid warfare

Many countries recognise the changes in the context of new challenges and threats, especially in the use of methods and where they occur. This is evident, for example, in the elaboration of

W. Gerasimov[1], who presented his model[2] in a form of a diagram that consists of six stages of the future conflict. The diagram shows a combination of military and non-military activities. He distinguishes the following phases:

– secret actions,
– situation exacerbation,
– the beginning of activities indicating conflict,
– crisis,
– solving,
– peace restoration.

The Finnish[3] elaboration includes six phases of actions:

– strategic preparation,
– political preparation,
– operational preparation,
– tension escalation,
– government overthrow central in the target region,
– alternative power establishment.

In comparison, the Latvian[4] National Defence Academy elaboration lists eight phases called: a new generation war, which include the following:

– nonmilitary actions having a negative impact on society, economic and political areas,
– actions aimed at misleading diplomatic, political and media centres,
– actions aimed at frightening the population and indicating the pointlessness of further resistance,
– destabilisation and propaganda,
– introduction of no-fly zone,
– the beginning of military operations by intensifying reconnaissance and the use of special forces,
– multidimensional, informational, diplomatic and military actions in order to exert pressure with the use of paramilitary and regular forces,
– destruction of enemy forces by special forces, precision strike and ground operations.

The lack of standardised studies in this field in the NATO and EU countries resulted in the necessity of working nationally[5].

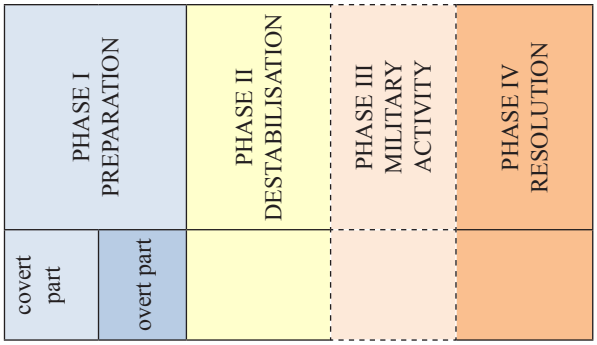
The project team analysed conflicts with hybrid elements, such as in Somalia, in Lebanon, in the east of Ukraine and action carried out by the Islamic State for the better understanding of these issues. All existing cases have been unified and function as universal hybrid warfare phases of action.

A detailed description of the phases is presented in appendix no. 2:

– preparation,
– destabilisation,
– military activity,
– resolution.

Table 1

The diagram of the phases of hybrid warfare



Source: own elaboration.

Activities at the preparation stage can be divided into two parts: covert and overt. The activities in the covert part are implicit. They may be characterised by the use of all sorts of ways to pressure and influence, led by corporations, NGOs or religious groups.

This phase is represented by the fact that the potential state, which is under attack, is not unaware of the fact that coordinated actions are carried out within it. Their importance is crucial when further actions are carried out by the aggressor.

When it comes to preparing these actions, they turn into an overt part when the target state notices the actions being taken against it.

[1] Валерий Герасимов – Chief of Staff Russian Federation

[2] Валерий Герасимов, Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

[3] Andras Racz, Russia's Hybrid War in Ukraine. Fiński Instytut Stosunków Międzynarodowych Raport 43 z 2015, s. 59–63.

[4] Janis Berzins, Russia's New Generation Warfare in Ukraine. Implications for Latvian Defence Policy National Defence Academy of Latvia. Policy Paper nr 2 z 2014, s. 6. for Techikinov i Bogdanov 2013, s. 15–22.

[5] The task of developing *The concept of contribution of Polish Armed Forces in countering hybrid threats*, commissioned by the Chief of General Staff of PAF.

In this part, one can see the phase of creating an atmosphere of financial meltdown inevitability, helplessness of government, weakness of security ministries and the possibility of armed conflict occurrence while maintaining current policy, both in the diplomatic and economic arena. The awakening of psychological and ideological separatism and ideological or religious aspirations take place.

The effective implementation of the development phase ensures the transition to the next - destabilisation phase. This is characterised by the disruption of the central and local centres of power, security structures, media and business, representatives, with the use of exploited methods and tools (political, economic, social, etc.) or cyber attack.

In this phase, one can specify the high scale of information activities - optional disinformation (at all levels: from strategic communications to local broadcasts) using all available means of communication in the area of possible conflict and in its international environment in order to achieve the desired reaction. If the main objective of the aggressor is only to destabilise certain areas (PEMSII) of the country, it means that these actions can be completed. If the aggressor's targets are not fully achieved, they can move onto the next phase - military activities.

At this stage, one can point out the formation of a local affiliates separatists group, made up of ethnic minorities or religious groups with the support of spiritual religious leaders, terrorist organisations, armed forces and special services of the aggressor.

Their main task is to stoke tension to confirm the helplessness of authorities and block possibilities of action by the ministries of power, e.g. the police and the army, and to take control of key facilities and areas which are necessary for affecting the success of the operation in a coordinated way. Objects of special significance include, border crossings, media relay stations, the key infrastructure such as crossroads, bridges and railway junctions and the airports. It should be emphasised that, at this stage, military activities are supported by coordinated and detailed planned diplomatic actions and expressed by information activities.

The last defined phase is resolution. It is characterised by the establishment of central and local authorities dependent on the aggressor. Resolution means mainly the acceptance of a forced political situation. If goals are not achieved, the phase of military activities may turn into open regular armed conflict. However, in this case, there are no hybrid activities/warfare any more.

Analytical model of hybrid warfare

Threats in the contemporary world are characterised by their diversity and the complexity of their occurrence. It is worth emphasising that national security[6] is not only the state but, above all, a dynamic process that is affected by a variety of determinants[7]. This results in difficulties in making a proper threat assessment. The complexity of its occurrence in certain areas radically affects the opportunity to find the appropriate methodology needed to determine the actual impact and what individual threats[8] mean.

The use of the method of modelling[9] is legit in this case. By creating models and confronting them with reality, among other things, through observations, one can check the occurring laws defining the phenomenon. Understanding this process is the inherent factor in predicting the course of events in the future[10]. This also applies to issues of national security. Anna Antczak-Barzan[11] states that "lack of ability to identify potential hazards in the long term based on developing internal and external trends (a close and further outlying state) can lead to disaster. Acting by focusing on only

[6] Security of the state – the actual state of internal stability and sovereignty of the state, which reflects the lack or presence of any threats (in the sense of existential basic needs and behavioural treatment of the public and the state as a sovereign subject in international relations). *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydanie szóste, AON, Warszawa 2002, s. 19.

[7] See the wider view: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 226.

[8] Threats - any disruptive effects on the subject, revealed in the form a crisis situation. See more widely: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

[9] Modelowanie matematyczne i badanie złożonych układów analitycznych. Maciej Rymanowski, Kraków 2007, s. 11.

[10] Ibidem.

[11] Professor of social science in the science of politics (Polish Academy of Sciences).

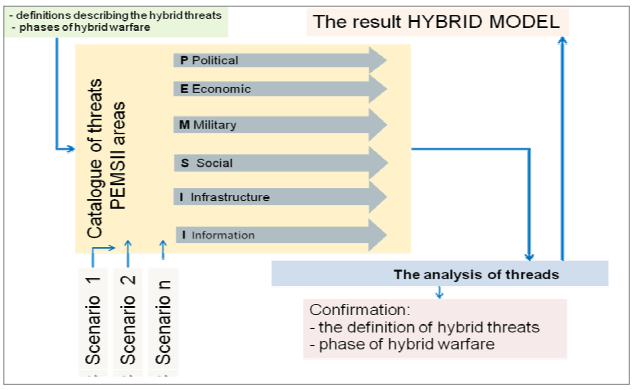
selected issues and taking care of particular private interests and the fight between different political factions have led more once to disaster"[12].

The findings above and the conclusions are the basis for discovering that the identified threats should be subjected to systematic analysis and monitoring. Currently, the analytical model of hybrid threats is designed to help to understand the symptoms and mechanisms of threats and allow to identify new ones that may significantly affect the functioning and the possibility of development of the state. In particular, they may be important for both internal and external safety. Such approach should also contribute to creating tools that would help counter potential threats.

While preparing an analytical model of hybrid warfare, certain assumptions have been adopted. Firstly, the work is carried out based on the PRINCE2[13] project management methodology. The aim of it was to use the principles of effective management that are required during the project, including the provision of a structured approach to ensure its success. However, even though this methodology provides knowledge about the techniques used, it does not specify in detail how to use them. Next is the input data. This includes: catalogue of threats in PEMSII areas, and the input data needed for definitions of hybrid threats and phases of hybrid warfare. In order to develop the analytical model, it has been assumed that environmental security will be divided into: political, economic, military, social, infrastructure and information areas. During the work, the project team defined characteristics separately as threads for each of these domains.

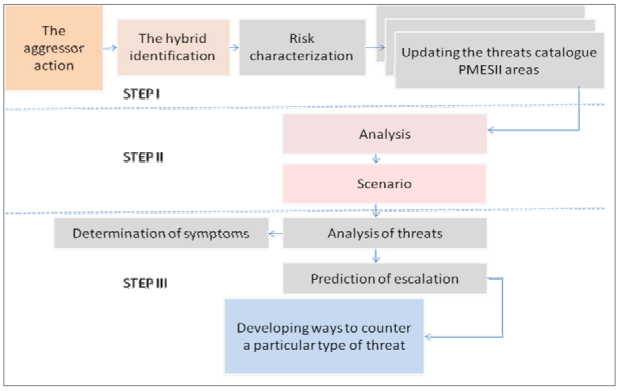
The idea of the model is illustrated in Figure 1.

During the development of the hybrid model, the following methodology of data processing was adopted (Fig. 2).



Source: own elaboration.

Figure 1. Schematic diagram of the analytical model of hybrid threats



Source: own elaboration.

Figure No. 2. Methodology of hybrid threats

At the first stage of the process, based on the risks arising from the actions of the aggressor, characterisation of threads takes place and they are put into catalogues. The second step requires selecting the most critical threat, to carry out the analysis and to develop case scenarios. These scenarios include all activities aimed at understanding the factors causing these risks and the creation of their symptoms and the relationship between them. During this stage, the threats are due to their:

– intentions: the interests, needs, politics, will,

– possibilities: the ability, methods, resources, constraints,

– historical data: assigned incidents, attempts, confirmed operations, frequency and effectiveness of these activities,

– signals: newly confirmed or anecdotal evidence.

This approach makes it possible to estimate the risk of threats. By risk estimation, it will be

[12] Translation from: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 238.

[13] PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009. Metodyka zarządzania projektami. Stosowana do sterowania i zarządzania projektami.

crucial to identify: the risks from a catalogue, the probability of the susceptibility of PEMSII areas and their impact and implications on the security of the state. It should be emphasised that the estimation values of the two basic parameters of the components - probability and effects – is significant in determining susceptibility to risk. The level of risk is estimated based on the use of a discreet grading scale of probability, which is included below (Tab. 2).

Table 2

Discreet probability grading scale

UNLIKELY	Threats previously unidentified and undocumented, which could occur only in exceptional and favourable circumstances. The value 0–20%
RARE	Threats are documented, risk symptoms or other circumstances are little known. The value of 20–40%
POSSIBLE	Threats are documented, symptoms or mechanism of formation is known. It can happen at a certain time in favourable conditions. The value of 40–60%
PROBABLE	Threats known and previously encountered. It is likely that in the case of a favourable environment they may occur in most circumstances. The value of 60–80%
VERY LIKELY	Threats are well known and systematic. There is a suitable environment for their creation. It is expected that these threats will happen in most circumstances. The value 80–100%

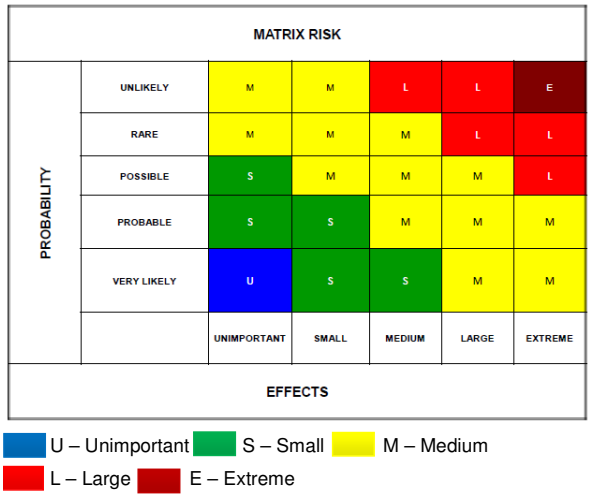
Source: Own study based on: *Ocena ryzyka na potrzeby zarządzania kryzysowego.* Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

The estimated value of the risk matrix reflects the relationship between probability and effects[14]. Each corresponds to the identified risk of one specific field (see Tab. 3).

In the more distant past, based on the vulnerability assessments of the risk for all identified threats, the resulting data is placed in a sheet classification, where they are grouped and evaluated in the area of PEMSII together with a description of their effects. According to the scale (Tab. 3), the risk is being prioritised from most to least important. In this case, one can distinguish two different approaches. The first one considers risks that have the highest probability of occurrence as the most important, and the other perceives the impact on the environment as the most important area.

Table 3

Risk matrix



Source: Own elaboration based on: Field Manual No. 5–19 (100–14), Composite Risk Management, Department of the Army. Washington, DC, July 2006 oraz Oceny ryzyka na potrzeby zarządzania kryzysowego. Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

This approach allows the threats to be linked together and also helps to identify the opportunities[15] and threats and to determine the trend. As a consequence, it may help in preventing and detecting the early symptoms, which in ordinary activities could remain unnoticed.

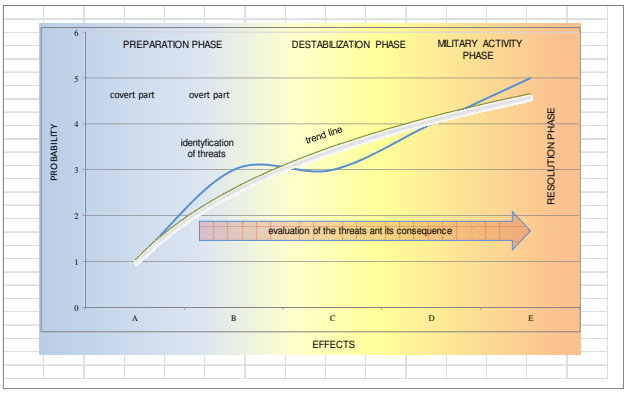
The presented model enables the identification of existing group challenges in environmental security, and specific opportunities and risks for the area. It reflects both the course and evolution of the risk, including the phases of hybrid warfare.

The following figure (Fig. 3) depicts an illustrative result of the threats positioned in the coordinate system where the x-axis shows the threat and the other shows the probability of the type of threat. The results clearly show the actions taken by the aggressor - determined using the blue curve. The full identification of the threats occurs by the time the breaking point is achieved by this threat. In addition, it allows the evaluation of threats in particular phases of the actions to be observed and the failure to adopt effective countermeasures. In

[14] Effect - the actual consequences of an action. Based on: PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009, s. 27.

[15] Opportunities - any circumstances for achieving the interest entity. Based on: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

addition, it allows the trend line to be determined. It is worth emphasising that such analysis makes it possible to develop strategies to combat threats.



Source: own elaboration.

Figure 3. Example output based on an analytical model of hybrid threats, one of the areas PEMSII

There is a slight resemblance in the studies of Anna Antczak-Barzan when it comes to methodology, by determining the opportunities and threats in the context of the examination of the Polish security environment.

She notices that a subjective selection of variables does not fully illustrate what lies behind the various opportunities and threats. She emphasises that, firstly, there is a need to pay more attention to threats rather than to focus on direct conclusions. According to the author, the final result depends on the number of opportunities and threats that could be identified in the area of each of the challenges and these can be various.

In addition, she indicates that the challenges themselves mean bigger risks rather than opportunities, and some of them are realistic because they have either already occurred, or, if the current rate remains maintained, it is almost certain that they will occur in the near future, and many potential chances arise when a number of conditions are met[16].

The desirability of the solutions adopted in the Polish analytical model of hybrid warfare and phases were confirmed by national and international experts in the working group in the framework of the Multinational Capability Development Campaign (MCDC).

[16] Based on: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 228.

Conclusion

The contemporary conflicts' hybridity should be seen as a conglomerate of all possible activities conducted by the aggressor or aggressors in PEMSII areas. Methods for countering these activities is not only the domain of the armed forces or non-military system, whose actual use takes place in the third phase of hybrid warfare. The definitions and hybrid warfare phases made it possible to put the events in chronological order. In addition, the analytical hybrid warfare model enables threats to be identified and points out the risk and potential escalation. Such activity makes it possible to figure out the threats countering strategy. However, it demands the engagement of all departments in order to achieve synergy, up-dating the threats catalogues bearing in mind the current multinational situation, the internal and external state of the country and their development trends in long-term strategy. The lack of capability to identify potential threats in the long term may consequently lead to non-reversible consequences.

Bibliography

Antczak-Barzan A., *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014.

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.

Валерий Герасимов. Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

Gruszczak A., *Hybrydowość Współczesnych Wojen – analiza krytyczna*. www. bbn.gov.

Hoffman F.G., *Hybrid Warfare and Challenges*, Joint Force Quarterly, JFQ Wyd. 51 2009.

Koziej S. i Brzozowski A., *Nauki o bezpieczeństwie: potrzeby i oczekiwania praktyki bezpieczeństwa narodowego. Tożsamość nauk o bezpieczeństwie*, Instytut Nauk Politycznych Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski, Wydawnictwo Adam Marszałek.

Materiały z prac grupy roboczej w ramach Wielonarodowej kampanii Rozwoju Zdolności (*Multinational Capability Development Campaign* – MCDC).

Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009.

Racz A., *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs, FIIA Report, Helsinki 2015.

Rymanowski M., *Modelowanie matematyczne i badanie złożonych układów analitycznych*, Kraków 2007.

Słownik wyrazów obcych PWN, Warszawa 1980. Por. Webster's New World Dictionary. wyd. 2. Prentice Hall Press. Nowy Jork 1986.

Sokala W., Zapała B., *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, Wydawnictwo BBN.

Zdrodowski B., *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014.

Appendix 1

TERMINOLOGY FROM THE ACTIVITIES OF HYBRID

This annex presents some definitions by. terminology developed by an expert group within the development *Concept of contribution of the Polish Armed Forces in countering the hybrid warfare.*

Hybrid warfare strategy

It guarantees achieving goals with the use of available capability and potential taking into account changes and trends in the environment. Depending on the plan phase of its implementation, it is conducted overtly or covertly using military and non-military instruments.

Hybrid activity/warfare

Actions that aim at achieving political and strategic goals with the possibility of maintaining previous economic and/or diplomatic relations. Hybrid warfare is conducted by state and/or non-state entities in a planned and coordinated way and it combines different ways of making pressure and making dependent on potential aggressor. All the actions can be conducted in a political, economic, military and social environment, including national, ethnic and religious minorities.

Hybrid warfare conduction

Generally accepted modus operandi that is restricted by potential aggressor's will and capabilities. It takes place in all or selected areas which are: political, economic, military, social, informational and infrastructural.

Appendix 2

PHASE I Preparation

1a covert part

Actions of this phase are covert due to its support and use of different types of pressure and influence groups. Their meaning is crucial for the preparation and conduction of further actions.

1b overt part

It takes place when hybrid warfare symptoms are exposed. The leading entity creates an atmosphere which is advantageous for goals achievement, not only in national, but also in international dimension.

PHASE II Destabilisation

Disorganization of centers of power and national/nations' security structures with the use of information tools available in all or selected areas, including political, economic and social spheres. This phase can be a target itself or include achieving other indirect goals.

PHASE III Military activity

The use and support of paramilitary and/or regular armed forces. The activity is often represented by non-military actions, including diplomatic and informational support.

PHASE IV Resolution

The acceptance of a resulting political situation