Krzysztof Liedel

Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?

Dynamika zmian w polskim środowisku bezpieczeństwa znacznie wzrasta w ostatnich latach. Wśród najważniejszych przyczyn takiego stanu rzeczy należy wymienić między innymi wyczerpującą się „premię bezpieczeństwa" wynikającą z zakończenia przed ćwierćwieczem zimnej wojny. W ciągu ostatnich 25 lat panowało bowiem przekonanie, że po zakończeniu napięć międzyblokowych ostatecznie odsunięto zagrożenie konfliktem militarnym na wielką skalę. Miało to przynieść ustabilizowanie się środowiska międzynarodowego w stopniu, który pozwoli na realną międzynarodową współpracę dla rozwoju, zamiast powtarzającego się w historii cyklu rywalizacji i konfliktów. Jako istotny czynnik wpływający na zmiany w polskim środowisku bezpieczeństwa trzeba ponadto wskazać pojawienie się nowych strategii i taktyk działania w przestrzeni międzynarodowej stosowanych przez aktorów działających w tym regionie.

Od 15 lat jesteśmy świadkami zmiany percepcji międzynarodowych zagrożeń bezpieczeństwa. W latach 90. XX w. panowało przekonanie, że doświadczenia II wojny światowej i zimnej wojny w dużym stopniu wyeliminowały zagrożenie klasycznym konfliktem o charakterze militarnym. Według niektórych badaczy miał nawet nastąpić „koniec historii"[1]. Był to okres zmian w środowisku międzynarodowym. Podjęto wówczas dyskusję na temat konieczności reformy Sojuszu Północnoatlantyckiego, który należało dostosować do nowego środowiska bezpieczeństwa. Środowiska, jak zakładano, pozbawionego wyzwań towarzyszących powstawaniu i ugruntowywaniu się pozycji NATO jako jednego z filarów globalnego ładu. Mogą o tym świadczyć choćby zapisy *Nowej doktryny strategicznej NATO* przyjętej podczas szczytu Sojuszu w Lizbonie w 2010 r., które opis środowiska bezpieczeństwa zaczynały od następującego stwierdzenia:

> Dzisiaj obszar euroatlantycki jest spokojny i zagrożenie terytorium NATO atakiem konwencjonalnym jest niewielkie. Jest to historyczny sukces polityki silnej obrony, euroatlantyckiej integracji i aktywnego partnerstwa, które wytyczały drogę NATO przez ponad pół wieku[2].

Z drugiej strony, przeciwwagą dla przekonania o „końcu historii" i koncepcji rosnącego bezpieczeństwa był rozwój zagrożeń o charakterze asymetrycznym, za którymi stali przede wszystkim aktorzy niepaństwowi, tacy jak międzynarodowe zorganizowane struktury przestępcze czy organizacje terrorystyczne. Bez wątpienia najważniejszym momentem zmiany w postrzeganiu tego, co stanowi największe zagrożenie dla współczesnych demokratycznych państw prawa, były wydarzenia z 11 września 2001 r. Atak na bliźniacze wieże World Trade Center dowiódł tego, że aktor niebędący państwem

[1] Pojęcie sformułowane przez Francisa Fukuyamę; był to również tytuł jego eseju napisanego w 1989 r., który został rozwinięty w książce *The End of History and the Last Man* wydanej w Stanach Zjednoczonych w 1992 r. W Polsce ukazały się dwie publikacje tego autora: *Koniec historii*, Poznań 1996 i *Ostatni człowiek*, Poznań 1997, które są tłumaczeniami fragmentów *The End of History…*

[2] *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie*, tłumaczenie robocze BBN [online], https://www.bbn.gov.pl/pl/wydarzenia/2694,KoncepcjaStrategicznaNATOtlumaczenie.html [dostęp: 22 IX 2015].

może wstrząsnąć globalnym ładem. Pokazał także, że nawet bez formalnej zmiany prawnomiędzynarodowych podstaw funkcjonowania (a zatem zmian w *Traktacie Północnoatlantyckim*) Sojusz Północnoatlantycki będzie nadal stanowił o kształtowaniu środowiska bezpieczeństwa. Po raz pierwszy bowiem w odpowiedzi na zagrożenie dla jednego z członków Sojuszu powołano się na *casus belli* zapisane w artykule 5 *Traktatu Północnoatlantyckiego*:

> Strony zgadzają się, że zbrojna napaść na jedną lub kilka z nich w Europie lub Ameryce Północnej będzie uważana za napaść przeciwko nim wszystkim; wskutek tego zgadzają się one na to, że jeżeli taka zbrojna napaść nastąpi, każda z nich, w wykonaniu prawa do indywidualnej lub zbiorowej samoobrony, uznanego przez Artykuł 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom tak napadniętym, podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami taką akcję, jaką uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego. O każdej takiej zbrojnej napaści i o wszystkich środkach zastosowanych w jej wyniku zostanie bezzwłocznie powiadomiona Rada Bezpieczeństwa. Środki takie zostaną zaniechane, gdy tylko Rada Bezpieczeństwa podejmie działania konieczne do przywrócenia i utrzymania międzynarodowego pokoju i bezpieczeństwa[3].

Zapisy te są tym istotniejsze, że – podobnie jak w przypadku *Karty Narodów Zjednoczonych* – trudno spodziewać się takiego rozwoju wydarzeń na arenie międzynarodowej, który pozwoliłby na realną zmianę traktatu, dostosowującą go do współczesnych wyzwań. Oznacza to, że w zbliżających się dziesięcioleciach będziemy opierać swoje bezpieczeństwo na zapisach aktu prawnomiędzynarodowego, który został powołany do życia w połowie ubiegłego wieku, a jego skuteczność będzie zależna od jego międzynarodowej interpretacji. Ta ostatnia zaś jest kwestią szczególnie istotną, biorąc pod uwagę przywołaną powyżej frazę (…) *podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami* ***taką akcję, jaką uzna za konieczną,*** *nie wyłączając użycia siły zbrojnej* (wyróżnienie własne autora).

Traktat Północnoatlantycki nie zobowiązuje zatem państw członkowskich do użycia siły wobec zagrożenia dla terytorium jednego lub więcej członków Sojuszu, lecz wymaga podjęcia kroków *uznanych za konieczne.* Jeśli więc dane państwo członkowskie uzna za konieczne udzielenie pomocy humanitarnej, i takiej udzieli, to wywiąże się ze swoich formalnych zobowiązań. Zasada *pacta sunt servanda* (w dobrej wierze!) chyba nigdzie nie jest tak istotna, jak w przypadku militarnego sojuszu obronnego opartego na tak sformułowanym *casus belli*.

Staje się to tym istotniejsze, im więcej nowych zagrożeń postrzegamy w swoim środowisku bezpieczeństwa. Konieczne wydaje się przypomnienie koncepcji sposobu kształtowania odpowiedniej percepcji zagrożenia i oceny stanu bezpieczeństwa sformułowanej przez Daniela Freia. Zdiagnozował on problem związany z postrzeganiem bezpieczeństwa, wskazując na cztery możliwe sposoby takiej percepcji:

1) stan braku bezpieczeństwa – występuje wtedy, gdy istnieje duże rzeczywiste zagrożenie zewnętrzne, a postrzeganie tego zagrożenia jest prawidłowe (adekwatne),

[3] *Traktat Północnoatlantycki*, Waszyngton, 4 IV 1949 r. [online], http://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pl [dostęp: 22 IX 2015].

2) stan obsesji – występuje w sytuacji, gdy nieznaczne zagrożenie jest postrzegane jako duże,
3) stan fałszywego bezpieczeństwa – występuje wówczas, gdy poważne zagrożenie zewnętrzne jest postrzegane jako niewielkie,
4) stan bezpieczeństwa – wstępuje wtedy, gdy zagrożenie zewnętrzne jest nieznaczne, a jego postrzeganie jest prawidłowe[4].

Koncepcja ta ma znaczenie w związku z problemami, jakie nastręcza nie tylko ocena, ale wręcz definiowanie zagrożeń w środowisku międzynarodowym oraz elastycznie sformułowane zobowiązanie wzajemnej pomocy, zapisane w przywołanym artykule 5 *Traktatu Północnoatlantyckiego*. Z tego właśnie względu rzadko kiedy dyskusja o kwestiach definicyjnych, toczona na poziomie akademickim, ma tak istotne znaczenie, jak dziś. *Realpolitik* już w połowie XIX w. została przez autora tego pojęcia określona jako (...) *prawo władzy rządzące państwami tak, jak prawo grawitacji rządzi światem fizycznym*[5]. I do tej „realności" polityki międzynarodowej, niezależnie od tego, jak bardzo jest zaskakująca, musimy się dziś odnosić. Jednym z elementów uprawiania tego typu polityki jest wykorzystywanie niebezpośrednich metod prowadzenia konfliktu, w tym konfliktu zbrojnego. Z całą pewnością można stwierdzić, że znakiem czasów jest konflikt hybrydowy.

Co jednak rozumiemy przez to pojęcie i do czego się ono odnosi? Oto pytania, z którymi warto się zmierzyć nie tylko ze względu na ciekawość naukową, lecz także z uwagi na dynamikę zdarzeń na arenie międzynarodowej, znacznie wyprzedzającą międzynarodowe porozumienia w dziedzinie bezpieczeństwa. Według analitycznego opracowania estońskiego Międzynarodowego Centrum Obrony i Bezpieczeństwa (International Centre for Defence and Security)[6], powołującego się na Franka Hoffmana, badacza zagadnień związanych z bezpieczeństwem międzynarodowym, w o j n a h y b r y d o w a (ang. *'hybrid warfare,*) to:

> (…) połączenie morderczości konfliktu międzypaństwowego i przedłużającej się żarliwości konfliktu nieregularnego. (…) Skomplikowane kampanie łączą operacje konwencjonalne o niskiej intensywności i operacje specjalne, działania ofensywne w cyberprzestrzeni oraz operacje psychologiczne wykorzystujące media społecznościowe i tradycyjne w celu wywierania wpływu na opinię publiczną, również na poziomie międzynarodowym[7].

Zdefiniowanie konfliktu (wojny hybrydowej) na potrzeby polskiego systemu bezpieczeństwa wzięło na siebie Biuro Bezpieczeństwa Narodowego. Na stronie BBN w opracowaniu *(Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa* czytamy:

---

[4] D. Frei, *Sicherheit. Grundfragen der Weltpolitik*, Stuttart 1977, s. 17−21, cyt. za: R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje − struktury − funkcjonowanie*, Warszawa 1999, s. 28−29.

[5] L. von Rochau, *Grundsätze der Realpolitik*, t. 1, Stuttgart 1853 [online], https://books.google.pl/books?id=c0hGAAAAcAAJ&pg=PP5 [dostęp: 22 IX 2015].

[6] Zob. http://www.icds.ee/.

[7] E. Hunter, P. Pernik, *The Challenges of Hybrid Warfare*, ICDS, kwiecień 2015 [online], http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf [dostęp: 22 IX 2015].

> Wojna hybrydowa [to] wojna łącząca w sobie jednocześnie różne możliwe środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp.[8]

Definicję wojny hybrydowej zaczerpniętą ze strony BBN warto uzupełnić innymi pojęciami z tegoż opracowania, które są niezbędne do pełnego zrozumienia zagrożeń wynikających z popularyzacji taktyk hybrydowych w działaniach państw. Szczególnie istotne w tym kontekście jest pojęcie a g r e s j i p o d p r o g o w e j . I tak, w *(Mini)Słowniku BBN* jest ona zdefiniowana następująco:

> Agresja podprogowa – działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa[9].

Warto w tym miejscu przywołać wspomnianą już wcześniej niedookreśloność artykułu 5 *Traktatu Północnoatlantyckiego*. W okolicznościach niesprzyjającego klimatu politycznego, przy umiejętnym stosowaniu przez potencjalnego agresora taktyk, które uniemożliwiają społeczności międzynarodowej jednoznaczne stwierdzenie, czy rzeczywiście ma już do czynienia z wojną, agresja podprogowa może stanowić jedno z najpoważniejszych zagrożeń współczesnego świata.

Kolejnym ważnym pojęciem, do którego zdefiniowania zmusza obecna sytuacja międzynarodowa, są z i e l o n e l u d z i k i . Choć zostało ono ukute w odniesieniu do rozwoju sytuacji na wschodniej Ukrainie i w związku z tym ma charakter bardzo potoczny, to odnosi się do zjawiska, które należy traktować jako niezwykle poważne zagrożenie. Zgodnie z przywoływanym już *(Mini)Słownikiem BBN*:

> „Zielone ludziki" – potocznie stosowane określenie uzbrojonych żołnierzy nieposiadających dystynkcji wojskowych, ani innych wyróżników, które pozwalałyby na określenie ich narodowości, prowadzących zbrojne działania regularne i nieregularne na terytorium wschodniej Ukrainy, wymierzone przeciwko jej integralności i niezawisłości[10].

Istotną cechą zagrożeń hybrydowych jest to, że przydatność omawianych taktyk jest różna w zależności od teatru działań, na jakim funkcjonuje państwo i jego potencjalny przeciwnik. Dowodem na to są chociażby wydarzenia na wschodniej Ukrainie.

Realizacja działań zaczepnych i ofensywnych jest możliwa w sytuacji spełnienia określonych warunków, np.: dużego zróżnicowania etnicznego, niedoskonałej kontroli terytorialnej i kontroli ruchu granicznego. Prawdopodobieństwo nieoczekiwanego pojawienia się na przykład w Polsce brygad „zielonych ludzików" jest znacznie mniejsze, niż

[8] *(Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa* [online], http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 22 IX 2015].

[9] Tamże.

[10] Tamże.

w przypadku państw mniej stabilnych. System obrony i bezpieczeństwa wewnętrznego RP sprawia, że Polska powinna być wyczulona na bardziej zaawansowane sposoby ataku stosowane w przypadku konfliktu hybrydywego.

Szczególne obszary potencjalnej walki w konflikcie hybrydowym, w których występuje konieczność podejmowania działań i przeciwdziałania zagrożeniom, a które zostały dostrzeżone w Polsce, to cyberprzestrzeń i infosfera. Walka informacyjna toczona zarówno w cyberprzestrzeni, jak i w mediach oraz problemy definicyjne i polityczne dotyczące konfliktu hybrydowego są jednymi z priorytetów w kwestii aktywnego przeciwdziałania zagrożeniom. W związku z tym są potrzebne działania dostosowawcze na poziomie prawnym i strategicznym. W Polsce tego rodzaju inicjatywa została podjęta już w 2014 r., kiedy to powstawały zręby przyjętej przez Radę Bezpieczeństwa Narodowego *Doktryny cyberbezpieczeństwa RP*.

Dokument ten, którego źródłami były zarówno *Strategia Bezpieczeństwa Narodowego*, jak i wyniki poprzedzającego jej przyjęcie *Strategicznego Przeglądu Bezpieczeństwa Narodowego*, stanowi, że:

> **Strategicznym celem** w obszarze cyberbezpieczeństwa RP, sformułowanym w Strategii Bezpieczeństwa Narodowego RP, **jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni**, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia[11].

Jeśli chodzi o infosferę i zapewnienie bezpieczeństwa informacyjnego RP, to zapisy o podobnym charakterze znalazły się w projekcie *Doktryny bezpieczeństwa informacyjnego RP*. Dokument ten, będący w końcu lipca 2015 r. jeszcze w opracowaniu, zawiera stwierdzenie, że:

> Celem strategicznym w obszarze bezpieczeństwa informacyjnego jest zapewnienie bezpiecznego funkcjonowania RP w przestrzeni informacyjnej, z uwzględnieniem bezpieczeństwa informacyjnego struktur państwowych (zwłaszcza administracji publicznej, służb bezpieczeństwa i porządku publicznego, służb specjalnych i sił zbrojnych), sektora prywatnego i społeczeństwa obywatelskiego[12].

Łatwo zauważyć, że podejście metodologiczne w obu dokumentach jest bardzo zbliżone i wynika z przywoływanego już *Strategicznego Przeglądu Bezpieczeństwa Narodowego*. Istotną wartością obu doktryn jest urealnienie i precyzyjne zdefiniowanie nowych wyzwań i zagrożeń. Nowych nie w sensie powstania niespotykanego dotąd rodzaju zagrożenia (gdyż taka konstatacja w stosunku do wojny informacyjnej stałaby w sprzeczności ze *Sztuką wojny* Sun Tzu), ale raczej w kontekście priorytetyzowania zadań i określania najważniejszych obszarów aktywności w zmieniającym się środowisku bezpieczeństwa. Trzeba bowiem podkreślić, że transsektorowość jest nie-

[11] *Doktryna cyberbezpieczeństwa RP* [online], https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, s. 9 [dostęp: 22 IX 2015]. Wyróżnienie w tekście oryginalnym.

[12] Projekt *Doktryny bezpieczeństwa informacyjnego RP*, lipiec 2015 r. [online], https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf, s. 5 [dostęp: 22 IX 2015].

odłączną cechą zagrożeń w cyberprzestrzeni i zagrożeń informacyjnych. Konieczność tworzenia i optymalizacji funkcjonowania stosownych fizycznych elementów systemu bezpieczeństwa narodowego i obrony (np. wyspecjalizowanych jednostek wojskowych oraz właściwych jednostek organizacyjnych służb specjalnych) staje się jednym z priorytetów organizacji systemu bezpieczeństwa narodowego, umożliwiającym jego efektywne funkcjonowanie.

Wykorzystywanie wielu środków, które mogą służyć realizacji celów operacyjnych i strategicznych w konflikcie hybrydowym, wymaga umiejętnego posługiwania się narzędziami, zwłaszcza tymi typowymi dla ochrony cyberprzestrzeni i infosfery. Nie tylko pozwalają one na ewentualne opanowanie systemu dowodzenia i kontroli przeciwnika, lecz także pomagają wywierać wpływ na szeroko pojętą opinię publiczną w kraju i za granicą. Przy założeniu, że jednym z najtrudniejszych aspektów zarządzania kryzysem wynikającym z zagrożeń hybrydowych jest aspekt komunikacji i wypracowania wspólnej świadomości sytuacyjnej, cyberprzestrzeń i infosfera stają się najbardziej prominentnymi polami prowadzenia walki i pierwszą linią starcia. Uważna obserwacja ruchów przeciwnika i system wczesnego ostrzegania prawidłowo funkcjonujący w tych właśnie dwóch obszarach będą stanowić o zdolności do prowadzenia działań prewencyjnych w innych wymiarach dotyczących bezpieczeństwa państwa i jego obywateli.

Wysiłki podejmowane przez jednostki administracji publicznej RP, których celem jest sformułowanie doktrynalnej odpowiedzi na nowe zagrożenia świadczą o tym, że zagrożenia związane z konfliktem hybrydowym są w Polsce dobrze rozpoznane.

Środowisko bezpieczeństwa RP, definiowane podczas Strategicznego Przeglądu Bezpieczeństwa Narodowego (SPBN), było postrzegane jako niezwykle złożone i dynamiczne już na etapie analiz prowadzonych w związku z tym przedsięwzięciem. Warto jednak podkreślić, że w *Białej Księdze Bezpieczeństwa Narodowego*[13], wydanej w 2013 r. jako podsumowanie SPBN, nie występują jeszcze takie terminy, jak „wojna hybrydowa" czy „agresja podprogowa".

Tym ważniejsze było sformułowanie odpowiednich definicji oraz wprowadzenie do debaty publicznej pojęć określających otaczającą nas rzeczywistość międzynarodową. Choć definicje te nie mają charakteru prawnomiędzynarodowego ani nawet prawnego w skali krajowego systemu prawa, to mogą stać się początkiem formułowania koncepcji odpowiedzi na takie zagrożenia. W przypadku Polski jest to o tyle istotne, że toczący się za naszą wschodnią granicą konflikt rosyjsko-ukraiński jest źródłem potencjalnych zagrożeń dla stabilności w regionie. Nie należy o tym zapominać nawet w sytuacji takich aktualnych wydarzeń, jak np. trwający od miesięcy kryzys imigracyjny, na który Europa nie znajduje dobrej recepty, gdyż zmiana geopolityczna wynikająca z ewolucji rosyjskiej polityki międzynarodowej pozostaje istotnym czynnikiem wpływającym na bezpieczeństwo RP i jej obywateli.

Konieczność dostosowania nie tylko uregulowań prawnych, lecz także przede wszystkim podstaw koncepcyjnych prowadzenia działań defensywnych oraz zaczepno-obronnych wymaga pełnej świadomości sytuacyjnej i realnej oceny środków, jakimi dysponuje przeciwnik, znajomości jego celów geostrategicznych oraz intencji w długiej perspektywie.

[13] *Biała Księga Bezpieczeństwa Narodowego RP*, Warszawa 2013.

W debacie publicznej pojawiają się głosy mówiące o tym, że wprowadzanie pojęcia „wojny hybrydowej" mija się z celem, ponieważ w historii ludzkości konflikty od zawsze były prowadzone wszelkimi dostępnymi środkami, które mogły zwiększyć prawdopodobieństwo osiągnięcia założonego celu. Część badaczy argumentuje więc, że zamiast koncentrować się na tworzeniu nowych pojęć, trzeba skupić się na wykrywaniu i definiowaniu złożonych kombinacji dostępnych środków walki tak, aby być gotowym na przeciwdziałanie im[14].

I choć z punktu widzenia taktyki wojskowej i operacji realizowanych na teatrze działań wojennych subtelne rozróżnienia pojęciowe mogą mieć nikłe znaczenie, to z punktu widzenia politycznego, w sytuacji potrzeby jasnego zdefiniowania międzynarodowych reakcji na zaistnienie aktu wojny, te definicje mogą stanowić o „być albo nie być" solidarności pomiędzy sojusznikami. Ta solidarność, a także wspólne, spójne obraz i ocena sytuacji mogą być niezmiernie ważne w przypadku potencjalnego konfliktu. Doktryna wojenna Federacji Rosyjskiej z 2014 r. daje szczególne powody do dbałości o tego rodzaju solidarność w kontekście zagrożeń hybrydowych. Jak bowiem warto przypomnieć, to właśnie w tym dokumencie pojawiają się następujące zapisy:

1. kompleksowe użycie sił zbrojnych, jak również politycznych, ekonomicznych, informacyjnych i innych środków niewojskowych, realizowanych przy szerokim wykorzystaniu potencjału protestu i sił operacji specjalnych,
2. wpływanie na przeciwnika na całej głębokości jego terytorium, w globalnej przestrzeni informacyjnej, w przestrzeni powietrzno-kosmicznej, na lądzie i morzu,
3. udział w działaniach wojennych nieregularnych formacji zbrojnych i prywatnych firm wojskowych,
4. stosowanie niebezpośrednich i asymetrycznych metod działań,
5. wykorzystanie sił politycznych i ruchów społecznych finansowanych i zarządzanych z zewnątrz[15].

Biorąc pod uwagę sformułowania tego dokumentu oraz jego usytuowanie prawno-polityczne nietrudno skonstatować, że (niezależnie od używania nomenklatury „hybrydowa") niestandardowa forma konfliktu wykorzystująca komponenty asymetryczne, informacyjne i niebezpośrednie stała się immanentną częścią rzeczywistości, w której funkcjonują współczesne państwa.

Analizując złożoność wykorzystywanych środków i sposobów walki, problemy z ich definiowaniem, małą intensywność potencjalnych wrogich działań (czyli działania poniżej progu agresji) oraz anonimowość sił biorących udział w ewentualnym konflikcie, sformułowanie sojuszniczej odpowiedzi zaczyna być kwestią decyzji politycznej, która zastępuje automatyzm wynikający z międzynarodowych porozumień obronnych. Stanowi to duże wyzwanie, zwłaszcza w związku z przywołanym zapisem *Traktatu* o tym, że państwa członkowskie Sojuszu mają reagować na potencjalną agresję przez podjęcie (…) *takiej akcji, jaką uzna*[ją] *za konieczną* – bez bezpośredniej wzmianki o bezwzględnym obowiązku udzielania pomocy zbrojnej.

[14] D. Van Puyvelde, *Hybrid war: does it even exist?* [online], http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm [dostęp: 22 IX 2015].

[15] J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle Doktryny Wojennej Rosji,* maj 2015 [online], http://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf [dostęp: 22 IX 2015].

Z tego powodu, niezależnie od puryzmu pojęciowego krytykującego wprowadzanie do obiegu sformułowań, takich jak „wojna hybrydowa", trzeba zgodzić z jednym: jakbyśmy tego stanu (nie)bezpieczeństwa nie nazwali, musimy być przygotowani do funkcjonowania w środowisku bezpieczeństwa, w którym konflikt mieszany, wykorzystujący wszystkie dostępne taktyki, strategie, metody i środki jest faktem. I nostalgia za czasami starcia klasycznego, jasno określonego granicami *ius in bello*, nie przywróci go prawdopodobnie już nigdy.