BIURO BEZPIECZEŃSTWA NARODOWEGO

Warszawa, 26 października 2012 r.

Szef Biura Bezpieczeństwa Narodowego
Stanisław Koziej

IDENTYFIKACJA ZAGROŻEŃ GLOBALNYCH DLA BEZPIECZEŃSTWA MIĘDZYNARODOWEGO

Nie ulega wątpliwości, że dzisiaj strategiczne środowisko bezpieczeństwa międzynarodowego podlega niezwykle dynamicznym zmianom. Pogłębia się zapoczątkowana na przełomie XX i XXI wieku deregulacja systemu budowanego w czasach zimnej wojny. Względna stabilizacja wypierana jest przez destabilizację. Wskutek kryzysu finansowego chwieją się fundamenty gospodarcze bezpieczeństwa. Nabierają znaczenia nowe wyzwania i zagrożenia. Wymienię choćby proliferację broni masowego rażenia, terroryzm globalny, cyberzagrożenia czy asymetryczne zagrożenia rakietowo-nuklearne. Mówiąc krótko: rośnie niepewność, nasilają się ryzyka.

Dalszą refleksję nad zagrożeniami i wyzwaniami dla bezpieczeństwa chciałbym poprzedzić uwagą, że są one kategoriami, przy pomocy których opisujemy środowisko (warunki) bezpieczeństwa. Dwoma pozostałymi tego typu kategoriami są szanse i ryzyka, którymi w swym wystąpieniu nie będę się bliżej zajmował, bo one nie są tematem naszej konferencji.

Dla porządku więc tylko zaznaczmy, że szanse rozumiemy jako niezależne od woli podmiotu okoliczności (zjawiska i procesy w środowisku bezpieczeństwa) sprzyjające realizacji interesów (misji) oraz osiąganiu celów w dziedzinie bezpieczeństwa. Z kolei ryzyka – to możliwości negatywnych dla danego podmiotu skutków własnego działania w sferze bezpieczeństwa. Obydwie te kategorie we współczesnych warunkach nabierają relatywnie coraz większego znaczenia.

Teoria i praktyka (wiedza i sztuka) wykorzystywania szans oraz redukowania ryzyka to szczególnie istotne, ale jednocześnie stosunkowo młode i czekające na pogłębione i szersze opracowanie dziedziny nowoczesnych strategii bezpieczeństwa narodowego i międzynarodowego. Na dzisiejszej konferencji nie zajmujemy się nimi bliżej, ale wierzę, że doczekają się one także należnego im wnikliwego zainteresowania ze strony środowisk naukowych, analityków i praktyków strategii.

Warto także już na początku podkreślić, że ważnym założeniem, którym kierujemy się w dyskusji nad bezpieczeństwem i którym kierowaliśmy się w pracach SPBN, jest

teza, że bezpieczeństwo i rozwój są niepodzielne, są nierozerwalnie ze sobą związane, wzajemnie od siebie zależne. Podkreślił to Prezydent RP w swoim przesłaniu.

Zauważmy, ze jest to w pełni zbieżne z głównym przesłaniem dzisiejszej konferencji: zagrożenia dla bezpieczeństwa są jednocześnie barierami dla rozwoju. AIe dodajmy od razu, że z kolei dobry rozwój stabilizuje bezpieczeństwo.

Chcę zwrócić uwagę, że chyba najbardziej praktycznym wyrazem związku bezpieczeństwa i rozwoju jest przyjęta u nas, z inicjatywy ówczesnego MON i obecnego Prezydenta Bronisława Komorowskiego, obowiązująca zasada ustawowego związania nakładów na wojsko z rozwojem gospodarczym. Wyraża się to w stałym wskaźniku 1,95% PKB przeznaczanego na budżet MON. Lepszy rozwój - lepsze warunki rozwoju sił zbrojnych, słabsze tempo przyrostu PKB – trudniejsze warunki dla sił zbrojnych.

Kompleksowe podejście do bezpieczeństwa zdeterminowało przyjętą w SPBN jego strukturę. Przyjęliśmy umowny podział problematyki bezpieczeństwa narodowego na dziedziny (obronną, ochronną, społeczną i gospodarczą), przy czym w dwóch pierwszych dominuje problematyka operacyjna (zapewnienia bezpieczeństwa), a dwóch ostatnich problematyka wsparcia (stwarzanie podstaw oraz warunków bezpieczeństwa). W ramach poszczególnych dziedzin wyróżniamy sektory bezpieczeństwa, a oprócz nich obszary transsektorowe (np. cyberbezpieczeństwo). Poszczególnym dziedzinom i sektorom podporządkowaliśmy podmioty bezpieczeństwa narodowego.

W ramach SPBN problematykę tę rozpatrywaliśmy w czterech analityczno-prognostyczno-projekcyjnych etapach obejmujących cztery obszary problemowe: analizę Polski jako podmiotu bezpieczeństwa, ocenę i prognozę strategicznych warunków bezpieczeństwa oraz opcjonalną projekcję strategii operacyjnej i opcjonalną projekcję strategii preparacyjnej.

Oceną zagrożeń i wyzwań zajmowaliśmy się w drugim etapie. Zagrożenie dla bezpieczeństwa to – mówiąc najogólniej - pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot. Jest to najbardziej klasyczny czynnik środowiska bezpieczeństwa.

W SPBN analizowaliśmy wiele rodzajów zagrożeń w różnych dziedzinach bezpieczeństwa. Na potrzeby tego wystąpienia zatrzymam się na zagrożeniach w dziedzinach obronnej i ochronnej, ograniczając się przy tym do jedynie trzech najbardziej wyraźnych zagrożeń transnarodowych o zasięgu globalnym: proliferacji broni masowego rażenia, terroryzmu oraz cyberzagrożeń.

Nie ulega wątpliwości, że szczególnie negatywne skutki dla świata niesie proliferacja broni masowego rażenia. Można ją sprowadzić do trzech „czarnych scenariuszy":

- „anarchii nuklearnej" w wyniku rozpadu globalnego reżimu nieproliferacji (opartego na Układzie o nieproliferacji broni jądrowej);
- destabilizacji państwa dysponującego bronią jądrową
- oraz uzyskania dostępu do środków nuklearnych przez podmioty niepaństwowe, w szczególności organizacje terrorystyczne.

W tym ostatnim przypadku technicznie najłatwiejsze może być wykorzystanie konwencjonalnego ładunku wybuchowego do rozpylenia materiałów radioaktywnych (tzw. brudna bomba).

Z proliferacją BMR ściśle wiąże się proliferacja technologii rakietowych, jako ważnego środka przenoszenia tej broni. Generuje to w rezultacie szczególnie groźne dzisiaj asymetryczne zagrożenia rakietowo-nuklearne. One właśnie głownie uzasadniają tezę o ukształtowaniu się już postklasycznej ery nuklearnej, a także przyspieszają rozwój obrony przeciwrakietowej.

Drugim istotnym zagrożeniem transnarodowym jest terroryzm. Stanowi on niebezpieczeństwo dla życia obywateli, stabilności demokratycznych instytucji, infrastruktury państwa oraz ładu międzynarodowego, w tym także w wymiarze globalnym.

Najbardziej dzisiaj rozpowszechnioną odmianę terroryzmu jest terroryzm motywowany radykalną ideologią islamską. Charakterystyczna dla niego jest próba przeniesienia swej aktywności do wnętrza świata zachodniego poprzez intensyfikację zjawiska terroryzmu rodzimego oraz inspirowanie prowadzenia tzw. indywidualnego dżihadu.

Inny co do motywów ideologicznych, jednak rodzący podobne skutki, jest odradzający się terroryzm skrajnie lewicowy, ultraprawicowy i nacjonalistyczno-separatystyczny. Stanowi on zagrożenie głównie dla krajów europejskich - ma swoje źródło m.in. w ideologiach ekstremistycznych, ksenofobii, niechęci do imigrantów, kryzysie ekonomicznym oraz niezadowoleniu społeczeństwa z działań podejmowanych przez rządy w tych sprawach. Większość ataków ugrupowań motywowanych tymi przyczynami wymierzonych jest w cele biznesowe i rządowe.

Mówiąc o terroryzmie nie sposób jeszcze raz nie podkreślić perspektywicznie szczególnie niebezpiecznej jego odmiany, jaką jest terroryzm z użyciem BMR, zwany też superterroryzmem. To najczarniejszy scenariusz, ale jednocześnie, niestety, coraz bardziej prawdopodobny. Dysponowanie taką bronią przez organizacje terrorystyczne może bowiem przybierać formę nie tylko fizycznego jej posiadania, ale także dywersyjnego włamywania się do istniejących systemów zabezpieczeń lub sterowania bronią nuklearną i uzyskiwania przez to dostępu do takiej broni.

W ten sposób przechodzimy do kolejnej formy terroryzmu, czyli cyberterroryzmu. Ale on jest częścią jeszcze szerszego problemu, jakim są w ogóle cyberzagrożenia.

Dotychczas terroryści wykorzystywali cyberprzestrzeń na szeroką skalę głównie do działań propagandowo-szkoleniowych i rekrutacyjnych. Ostatnio obserwujemy tendencję do podejmowania w niej działań stricte operacyjnych (atakowanie sieci teleinformatycznych i systemów technologicznych mających strategiczne znaczenie dla państw).

Warto podkreślić, że ataki cybernetyczne i operacje na szerszą skalę mogą podejmować zarówno grupy przestępcze, terrorystyczne, jak i państwa w ramach szeroko rozumianej wojny informacyjnej.

Można stwierdzić, że w zasadzie wszystkie rodzaje niebezpieczeństw istniejących w tradycyjnej, fizycznej geoprzestrzeni będą mieć swoje odpowiedniki w cyberprzestrzeni. Niedawno sami doświadczaliśmy takich form, jak np. cyberprotesty czy cyberdemonstracje. Takie kategorie, jak cyberagresja, cyberodstraszanie, cyberwojna już czekają na swoje szerokie opracowanie teoretyczne oraz praktyczne ich uwzględnianie w strategiach bezpieczeństwa.

Chciałbym teraz przejść do wyzwań w dziedzinie bezpieczeństwa. Rozumiem je jako sytuacje problemowe w dziedzinie bezpieczeństwa generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw bezpieczeństwa.

Wyzwania – inaczej niż zagrożenia – stwarzane są raczej przez partnerów i sojuszników niż przez przeciwników. W tym sensie zatrzymam się nad trzema wyzwaniami globalnymi, jakie dzisiaj stwarzają reorientacja strategiczna Stanów Zjednoczonych oraz ewolucja NATO i kłopoty UE.

Reorientacja strategiczna Stanów Zjednoczonych przyjmuje postać ich zwrotu w stronę Azji i Pacyfiku. Oznacza to, według Stanów Zjednoczonych, zmianę zimnowojennego paradygmatu, który umiejscawiał globalną rywalizację na linii Wschód-Zachód w Europie. Zwrot ten został ujęty w strategii obronnej USA ze stycznia 2012 r., a także w pewnym sensie w koncepcji tzw. „kierowania z tylnego siedzenia" - po raz pierwszy zastosowanej w praktyce przez Waszyngton podczas operacji libijskiej. Oznacza on przede wszystkim przeniesienie zainteresowania strategicznego oraz częściowo także wysiłku wojskowego. Przed europejskimi członkami NATO pojawia się nowe wyzwanie – Europa musi bardziej niż dotychczas wziąć sprawy bezpieczeństwa europejskiego w woje ręce.

Co do ewolucji NATO to można postawić tezę, że zakończyła się pozimnowojenna faza transformacji Sojuszu i pojawia się konieczność zdefiniowania nowego paradygmatu tej transformacji.

Przez ostatnie 20 lat Sojusz dostosowywał się do radykalnie i szybko zmieniającego się środowiska bezpieczeństwa głównie kosztem swej podstawowej, obronnej funkcji opartej o art. 5 TW. NATO angażowało się w operacje poza swoim terytorium traktatowym, pozostawiając na dalszym planie zadania jego obrony. Był to model „rozwoju przez redukcję", rozwoju jednej funkcji za cenę innej: poszerzania funkcji pozatraktatowej kosztem redukcji fundamentalnej funkcji traktatowej. Przykładem jest zaangażowanie NATO w Afganistanie.

W ostatnim czasie można zaobserwować potrzebę reorientacji strategicznej Sojuszu. Przesunięcie strategicznego zainteresowania USA z Europy do Azji niesie konsekwencje dla Europy, które można wyrazić następującym zdaniem: skoro Amerykanie przenoszą się z Europy do Azji, my musimy wracać z Azji do Europy. Jednym słowem, wśród europejskich państw maleje zainteresowanie operacjami poza obszarem traktatowym Sojuszu. Ale jednocześnie trudno sobie wyobrazić, aby NATO mogło w ogóle uchylić się od tego typu zadań. I na tym polega główne wyzwanie strategiczne, w tym transformacyjne, przed jakim stoi obecnie Sojusz. Streszcza je pytanie: jakie ma być postafgańskie NATO?

Istotę nowego modelu transformacji NATO, jaki w wyniku tego wyzwania zaczyna, a przynajmniej powinien zacząć się kształtować, można sprowadzić do frazy: „najpierw dom" (home first).

Nową erę charakteryzować winna przede wszystkim konsolidacja. Od ekspansji do konsolidacji – tak można skrótowo określić zwrot strategiczny, w którego obliczu stoi obecnie NATO. Jeśli Sojusz chce mieć swobodę operowania poza obszarem traktatowym, najpierw musi zapewnić poczucie bezpieczeństwa państw członkowskich na swoim terytorium. To jest warunek podstawowy. Jeśli chcemy gdzieś się angażować, to najpierw musimy być bezpieczni w domu. To jest konieczny warunek skuteczności strategicznej NATO w nowym środowisku bezpieczeństwa.

Jeszcze jedno wyzwanie należy na koniec mocno podkreślić. To dylemat bezpieczeństwa w ramach UE. Są z nim znane kłopoty. W dużym stopniu determinowane kryzysem gospodarczym. Ale nie tylko. Ważnym powodem jest w dużej mierze już przestarzały fundament koncepcyjny, jakim jest strategia bezpieczeństwa UE. To rdzewiejący coraz bardziej drogowskaz strategiczny z 2003 roku. Trzeba go uaktualnić. Potrzebna jest nowelizacja strategii bezpieczeństwa UE. BBN podejmuje już od dłuższego czasu stosowne inicjatywy w tym względzie. Ale wciąż jeszcze brak wyraźnej woli politycznej dużej części państw UE, aby ten proces uruchomić. To wyzwanie o dużym znaczeniu dla bezpieczeństwa nie tylko Europy, ale także w wymiarze globalnym.

* * *

W zakończeniu chciałbym wspomnieć, że w SPBN syntetyzując wszelkie prawdopodobne zagrożenia, wyzwania, ryzyka i szanse dla bezpieczeństwa przyjęliśmy trzy możliwe scenariusze kształtowania się przyszłego środowiska bezpieczeństwa:

1. Scenariusz integracyjny, optymistyczny – zakładający przewagę pozytywnych trendów nad negatywnymi; przewagę szans i możliwości podejmowania wyzwań nad zagrożeniami i ryzykami;
2. Scenariusz dezintegracyjny, pesymistyczny – zakładający z kolei przewagę negatywnych tendencji dezintegracji istniejącego systemu bezpieczeństwa nad pozytywnymi; przewagę zagrożeń i ryzyk nad szansami i możliwościami pozytywnego podejmowania wyzwań;
3. Scenariusz ewolucyjny, realistyczny – zakładający względną równowagę tendencji i procesów negatywnych i pozytywnych.