

Warszawa, 8 lipca 2015 r.

DEKALOG PRIORYTETÓW STRATEGICZNYCH W DZIEDZINIE BEZPIECZEŃSTWA NARODOWEGO RP

Stanisław Koziej, szef Biura Bezpieczeństwa Narodowego

W ostatnich latach doszło do pogorszenia warunków bezpieczeństwa w bezpośrednim otoczeniu Polski. Za wschodnią granicą trwa konflikt wojenny. Rosja, dokonując nielegalnej aneksji Krymu, a następnie wspierając pośrednio i bezpośrednio separatystyczną rebelię na wschodzie Ukrainy, podważyła porządek międzynarodowy w Europie. Jednocześnie na Bliskim Wschodzie i w Afryce Północnej rozszerza się zagrożenie ze strony tzw. Państwa Islamskiego, a terroryzm wewnątrz europejski osłabia stabilność zjednoczonej Europy. Wszystko to powoduje określone zagrożenia i wyzwania dla bezpieczeństwa, które wymagają zarówno bieżących, jak i długoterminowych wysiłków na rzecz wzmocnienia systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej. W niniejszej analizie proponuję dziesięć strategicznych priorytetów, których realizacja powinna prowadzić do osiągnięcia tego celu.

Najpilniejszym i bieżącym zadaniem jest dokończenie procesu zmian w systemie bezpieczeństwa Polski związanych ze strategicznym zwrotem przenoszącym priorytety z misji zagranicznych (polityki ekspedycyjnej) w kierunku zadań dotyczących bezpośredniego bezpieczeństwa Polski, w tym obrony własnego terytorium. Wymaga to od instytucji państwa szeregu wzajemnie skoordynowanych działań, ukierunkowanych na wzmocnienie narodowego potencjału, a także wzmacnianie zewnętrznych filarów bezpieczeństwa Polski.

Zgodnie z tym, pierwszym, bieżącym priorytetem jest:

1. dokończenie prac nad uaktualnieniem narodowych planów operacyjnych i programów rozwojowych (preparacyjnych) oraz zakończenie tego cyklu strategicznego weryfikacją funkcjonowania systemu bezpieczeństwa w ramach ćwiczenia KRAJ, a następnie rozpoczęcie kolejnego Strategicznego Przeglądu Bezpieczeństwa Narodowego.

W ten sposób rozpocznie się kolejny cykl planowania strategicznego, w którym priorytetami powinny być:

2. konsolidacja i ponadresortowa integracja systemu kierowania bezpieczeństwem narodowym;
3. budowa systemu strategicznej odporności kraju na agresję;
4. organizacja narodowego systemu bezpieczeństwa informacyjnego, w tym przyspieszenie budowy systemu cyberbezpieczeństwa;

5. doskonalenie systemu przygotowywania rezerw mobilizacyjnych, wraz z przeprowadzeniem reformy Narodowych Sił Rezerwowych;
6. wdrożenie „trzeciej fali” modernizacji technicznej Sił Zbrojnych RP (cyberobrona, systemy bezzałogowe, broń precyzyjnego rażenia);
7. uruchomienie i realizacja Narodowego Programu Systemów Bezzałogowych, będącego kołem zamachowym innowacyjności krajowego potencjału naukowo-przemysłowego;
8. działania wzmacniające Sojusz Północnoatlantycki;
9. działania prowadzące do strategicznego upodmiotowienia UE i rozwoju współpracy NATO-UE (polityczno-strategiczna odpowiedź na zagrożenia hybrydowe);
10. umacnianie strategicznych partnerstw, szczególnie sojuszu z USA.

1. Realizacja narodowego planowania strategicznego

Zadanie: dokończenie cyklu planowania strategicznego, przy uwzględnieniu negatywnych zmian w środowisku bezpieczeństwa spowodowanych agresywną polityką Rosji; weryfikacja jego rezultatów w ćwiczeniu typu KRAJ oraz uruchomienie kolejnego cyklu planistyczno-organizacyjnego, rozpoczynając od przeprowadzenia drugiego Strategicznego Przeglądu Bezpieczeństwa Narodowego.

W ostatnich latach uporządkowano działania państwa w obszarze narodowego planowania strategicznego. Obecnie kończy się jego pełny cykl, rozpoczęty pierwszym Strategicznym Przeglądem Bezpieczeństwa Narodowego (w latach 2010–2012) a następnie zatwierdzeniem nowej Strategii Bezpieczeństwa Narodowego RP (listopad 2014 r.). W bieżącym roku wskazane jest dokończenie cyklu.

Po wydaniu Polityczno-Strategicznej Dyrektywy Obronnej RP, co powinno nastąpić w możliwie najbliższym czasie, należy uaktualnić plany operacyjne funkcjonowania wszystkich struktur państwa w czasie zagrożenia i wojny. Dotyczy to zarówno urzędów centralnych i samorządów, jak też Sił Zbrojnych i pozostałych służb oraz straży wykonujących zadania na rzecz bezpieczeństwa. Wiąże się z tym także potrzeba aktualizacji Planu Reagowania Obronnego RP.

Kolejnym zadaniem jest przygotowanie i przeprowadzenie systemowego ćwiczenia weryfikacyjnego pod kryptonimem KRAJ. Koncepcja ćwiczenia powinna być zatwierdzona po wydaniu Polityczno-Strategicznej Dyrektywy Obronnej RP. Podczas ćwiczenia w roli Naczelnego Dowódcy Sił Zbrojnych powinna po raz pierwszy wystąpić osoba wskazana do powołania na tę funkcję w razie wojny.

Równoległe z przygotowaniem operacyjnymi należy uruchomić i przeprowadzić kolejny cykl programowania rozwojowego Sił Zbrojnych RP, rozpoczynając od wydania Postanowienia Prezydenta RP w sprawie Głównych Kierunków Rozwoju Sił Zbrojnych RP oraz ich Przygotowań do Obrony Państwa na lata 2017–2026.

Na początku 2016 r. wskazane jest uruchomienie kolejnego cyklu narodowego planowania strategicznego, rozpoczynając od przeprowadzenia drugiego Strategicznego Przeglądu Bezpieczeństwa Narodowego. Przegląd powinien mieć weryfikacyjno-koncepcyjny charakter,

dając podstawę do zaprojektowania rekomendacji odpowiadających zmieniającym się warunkom bezpieczeństwa międzynarodowego i narodowego.

Przegląd powinien sformułować rekomendację w sprawie utrzymania, nowelizacji lub przygotowania nowej Strategii Bezpieczeństwa Narodowego RP. Efektem Przeglądu, obok opracowania raportu dla władz państwa, powinno być także wydanie drugiej Białej Księgi Bezpieczeństwa Narodowego RP.

Przegląd może być też okazją do podjęcia prac nad pierwszą w Polsce Encyklopedią Bezpieczeństwa Narodowego, wspierającą rozwój polskich nauk o bezpieczeństwie.

2. Konsolidacja (integracja) systemu kierowania bezpieczeństwem narodowym

Zadanie: wzmocnienie organizacyjne systemu kierowania bezpieczeństwem narodowym - utworzenie Komitetu Rady Ministrów ds. Bezpieczeństwa Narodowego i wzmocnienie Rządowego Centrum Bezpieczeństwa (RCB), jako ciała sztabowego tego komitetu. Przeprowadzenie treningu strategicznego z Naczelnym Dowódcą SZ, weryfikacja stanowisk kierowania obroną państwa, zapewnienie bezpiecznej łączności oraz zakup samolotów do przewozu najważniejszych osób w państwie (w tym jako mobilnych stanowisk kierowania).

Bezpieczeństwo Polski jest wciąż zarządzane „resortowo”. Istnieją odrębne systemy planowania i zarządzania reagowaniem obronnym oraz kryzysowym sięgające od centrali, przez resorty, województwa, aż do samorządów (odrębne plany i programy obronne, kryzysowe, Obrony Cywilnej Kraju). Brakuje zintegrowanego oraz kompleksowego podejścia (*comprehensive approach*).

Dzieje się to w warunkach, gdy coraz więcej dziedzin bezpieczeństwa ma charakter transsektorowy (np. cyberbezpieczeństwo, bezpieczeństwo energetyczne, sprawy przemysłu obronnego, koordynacja służb specjalnych itp.), co wymaga ujednoczonego zarządzania. Jednocześnie kompleksowo uregulowana powinna zostać m.in. kwestia organizacji i funkcjonowania Obrony Cywilnej Kraju, jako struktury odpowiedzialnej za ochronę ludności w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.

Dlatego istnieje potrzeba konsolidacji systemu kierowania bezpieczeństwem narodowym na wszystkich szczeblach państwa – od Rady Ministrów do poziomu samorządowego – według modelu: decydujący, kolegialny organ doradczy, organ sztabowy.

Na szczeblu centralnym wskazane jest ustanowienie Rządowego Komitetu ds. Bezpieczeństwa Narodowego z obsługującym go Rządowym Centrum Bezpieczeństwa Narodowego, powstałym przez rozwinięcie istniejącego obecnie RCB.

Należy także merytorycznie zintegrować główne dokumenty strategiczne w państwie dotyczące bezpieczeństwa. Na przykład zamiast obecnej Polityczno-Strategicznej Dyrektywy Obronnej, regulującej jedynie sprawy obronne, należałoby wydawać Polityczno-Strategiczną Dyrektywę Bezpieczeństwa Narodowego, regulującą działania państwa we wszystkich obszarach bezpieczeństwa.

Integrowanie systemu kierowania bezpieczeństwem narodowym wymaga również uporządkowania przepisów prawnych, co można osiągnąć poprzez przygotowanie ustawy dotyczącej kierowania bezpieczeństwem narodowym.

Realizacja tak kompleksowego podejścia w praktyce wymaga odpowiedniego przygotowania specjalistycznego kadr urzędniczych. Dla potrzeb systemu kierowania bezpieczeństwem

narodowym wskazane jest utworzenie uczelni akademickiej zajmującej się badaniami naukowymi i kształceniem w dziedzinie zintegrowanego, transsektorowego, ponadresortowego, ogólnopaństwowego bezpieczeństwa narodowego (zarówno kształceniem studentów, jak i – na specjalnych kursach – kadry kierowniczej i urzędniczej). Uczelnia taka mogłaby powstać przy okazji reformy wyższego szkolnictwa wojskowego.

3. Budowa systemu strategicznej odporności kraju na agresję

Zadanie: dokończenie opracowania i wdrożenie programu wzmocnienia strategicznej odporności kraju na agresję (zadania Wojsk Specjalnych w obronie kraju, reforma Narodowych Sił Rezerwowych, systemu rezerw mobilizacyjnych, Obrony Cywilnej Kraju, powszechność przygotowań obronnych, edukacja dla bezpieczeństwa, wspieranie inicjatyw i aktywności stowarzyszeń proobronnych oraz innych organizacji społecznych, w tym na rzecz krzewienia patriotyzmu).

Podstawą dla zapewnienia bezpieczeństwa zewnętrznego państwa jest odpowiedni potencjał odstraszenia, który może mieć wymiar zarówno ofensywny (odwetowy), jak i defensywny (zniechęcający).

W zakresie odstraszenia ofensywnego należy maksymalnie korzystać z potencjału sojuszniczego (nuklearnego i konwencjonalnego) i selektywnie budować własne zdolności. Jednocześnie Polska powinna organizować własny, narodowy system defensywnego odstraszenia (zniechęcania, powstrzymywania).

Celem działania tego systemu powinno być uodpornienie państwa oraz jego terytorium na różne formy agresji, w szczególności na agresję hybrydową, w tym zwłaszcza agresję podprogową (poniżej progu otwartej, regularnej wojny) tak, aby w kalkulacjach strategicznych potencjalnego agresora działania ofensywne były zbyt kosztowne w stosunku do spodziewanych korzyści politycznych i strategicznych.

Dlatego należy kontynuować budowę systemu strategicznej odporności kraju na wszelkiego rodzaju zagrożenia. Ideą tego systemu jest skoordynowanie działań (legislacyjnych, operacyjnych, szkoleniowych, organizacyjnych, technicznych itp.) w obszarach takich, jak:

- działania nieregularne na terytorium zajęтым przez przeciwnika;
- militarne i niemilitarne wsparcie wojsk operacyjnych w działaniach regularnych;
- przygotowywanie rezerw mobilizacyjnych;
- operacyjne przygotowanie terytorium i ochrona obiektów infrastruktury krytycznej;
- zapewnienie bezpieczeństwa obywateli i struktur państwa, w tym powszechna ochrona ludności;
- prowadzenie powszechnej edukacji dla bezpieczeństwa, w tym obronne przygotowanie społeczeństwa, m.in. przez wykorzystanie potencjału pozarządowych organizacji proobronnych.

Stosownie do powyższych zadań operacyjnych powinny zostać doprecyzowane zadania Wojsk Specjalnych, zreformowanych Narodowych Sił Rezerwowych (NSR), niewojskowych formacji bezpieczeństwa i ochrony ludności czy pozarządowych organizacji proobronnych. To także zadania związane z doskonaleniem systemu rezerw mobilizacyjnych.

Działania nieregularne na terytorium zajęтым przez przeciwnika powinny być organizowane i koordynowane przez Wojska Specjalne. W związku z tym konieczne jest ich szersze ukierunkowanie zadaniowe na obronę kraju; zwiększenie liczebności oraz ich szkolenie na terytorium kraju z pozostałymi strukturami państwa.

Zadaniem zreformowanych Narodowych Sił Rezerwowych powinno być lokalne wspieranie działań wojsk operacyjnych i innych sił bezpieczeństwa, a także uczestniczenie w działaniach nieregularnych na terytorium opanowanym przez przeciwnika. Przygotowanie do realizacji tego zadania powinno opierać się na zreformowaniu NSR tak, aby stanowiły one odrębne formacje przy jednostkach wojskowych, przewidziane w operacyjnej podporządkowanie Wojewódzkich Sztabów Wojskowych („wojsko wojewodów”). Ważne, aby w ich skład wchodził przede wszystkim rezerwiści, a nie kandydaci do służby zawodowej.

Konieczne jest udoskonalenie systemu rezerw mobilizacyjnych, umożliwiających strategiczne rozwinięcie sił zbrojnych do wielkości i struktury czasu wojny oraz ich uzupełnianie w toku ewentualnych działań wojennych. Zadania w tym zakresie to odpowiednie zaplanowanie potrzeb, zorganizowanie zasobów mobilizacyjnych oraz ich systematyczne szkolenie.

Zapewnianie bezpieczeństwa struktur państwa, obywateli i infrastruktury krytycznej przed zagrożeniami zbrojnymi zapewniać powinny niewojskowe formacje bezpieczeństwa. Wiąże się to z koniecznością odpowiedniego doprecyzowania zadań oraz przygotowania Policji, służb specjalnych, straży samorządowych czy agencji ochroniarskich i formacji ochrony obiektów.

Za ochronę ludności cywilnej przed skutkami zagrożeń militarnych i niemilitarnych w czasie wojny powinny odpowiadać odpowiednio przygotowane formacje ochrony ludności. Zadania preparacyjne (przygotowawcze) w tej dziedzinie powinny polegać m.in. na stworzeniu systemu ratowniczego z udziałem służb takich, jak Państwowa Straż Pożarna czy pogotowie ratunkowe, wykorzystaniu w systemie ratownictwa Ochotniczych Straży Pożarnych oraz stworzenie struktur Obrony Cywilnej Kraju na czas wojny (stosowne przeformowanie na ten czas niektórych formacji służb ratowniczych w formacje Obrony Cywilnej Kraju).

Istotną rolę w systemie powinny pełnić społeczne organizacje proobronne (stowarzyszenia, klasy mundurowe, grupy rekonstrukcyjne), realizujące zadania przygotowania obywateli i społeczności lokalnych dla bezpieczeństwa państwa oraz przygotowania ich do działania w warunkach zagrożenia i wojny, w tym realizacji zadań obronnych.

4. Organizowanie narodowego systemu bezpieczeństwa informacyjnego, w tym przyspieszenie budowy systemu cyberbezpieczeństwa

Zadanie: opracować doktrynę bezpieczeństwa informacyjnego oraz zorganizować jednostki operacji w cyberprzestrzeni w Ministerstwie Obrony Narodowej oraz w innych resortach (np. Ministerstwie Spraw Wewnętrznych, Ministerstwie Administracji i Cyfryzacji) i służbach ochrony bezpieczeństwa publicznego, a także stworzyć system ponadresortowej koordynacji działań informacyjnych i w cyberprzestrzeni.

W ramach hybrydowych zagrożeń dla bezpieczeństwa Polski na pierwsze miejsce wysuwa się presja polityczno-militarna, realizowana głównie w sferze informacyjnej, także w cyberprzestrzeni. Dlatego priorytetem powinna być budowa skutecznego systemu bezpieczeństwa informacyjnego z dobrze zorganizowanym sektorem cyberbezpieczeństwa.

Początkiem działań powinno być opracowanie i przyjęcie doktryny bezpieczeństwa informacyjnego, jako jednego z dokumentów wykonawczych do Strategii Bezpieczeństwa

Narodowego RP. Doktryna powinna precyzować cele strategiczne, a także określać pożądane kierunki działań (zadania operacyjne) i niezbędnych przygotowań (zadania preparacyjne) w dziedzinie bezpieczeństwa informacyjnego.

Zgodnie z nakreślonymi wytycznymi, należy stworzyć i rozwinąć jednostki bezpieczeństwa informacyjnego (w tym cyberbezpieczeństwa) w obronnych i ochronnych (militarnych i pozamilitarnych) ogniwach systemu bezpieczeństwa narodowego. Powinny to być struktury zdolne do realizacji zadań zarówno o charakterze defensywnym, jak i ofensywnym.

Szczególnie istotne jest także zapewnienie suwerennego panowania operacyjnego oraz technicznego nad wysoce z informatyzowanymi systemami walki i wsparcia, w tym systemami kierowania (dysponowanie kodami źródłowymi ich oprogramowania). Ważnym zadaniem jest ponadresortowa koordynacja tej problematyki w ramach budowania zintegrowanego systemu kierowania bezpieczeństwem narodowym.

W kontekście zagrożeń w cyberprzestrzeni ważne jest:

- o wypracowanie mechanizmów wzajemnego oddziaływania i współpracy między sektorem publicznym a prywatnym;
- o zapewnianie równowagi między środkami bezpieczeństwa a swobodami obywatelskimi;
- o ciągłe podnoszenie świadomości obywatelskiej w zakresie cyberbezpieczeństwa;
- o wykorzystanie potencjału obywateli w ramach cyberobrony i cyberochrony kraju w formie wolontariatu dla cyberbezpieczeństwa państwa;
- o budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa, realizowanych we współpracy ze światem nauki oraz z przedsiębiorstwami komercyjnymi;
- o inwestowanie w narodowe rozwiązania w dziedzinie cyberbezpieczeństwa, w szczególności w dziedzinie kryptologii;
- o stworzenie krajowego mechanizmu koordynacji działań, służącego nie tylko usprawnieniu współpracy w ramach administracji publicznej, ale także koordynacji współpracy z sektorem prywatnym.

Obok działań w ramach bezpieczeństwa informacyjnego należy dążyć także do wzmocnienia innych pozamilitarnych obszarów bezpieczeństwa, w tym bezpieczeństwa energetycznego czy bezpieczeństwa ekonomicznego.

5. Doskonalenie systemu przygotowywania rezerw mobilizacyjnych oraz reforma Narodowych Sił Rezerwowych

Zadanie: rozwinąć system mobilizacji sił zbrojnych, z jednoczesną reformą Narodowych Sił Rezerwowych oraz włączeniem do niego aktywności społecznych organizacji proobronnych.

W warunkach posiadania przez państwo armii zawodowej konieczne jest dysponowanie odpowiednio licznymi i dobrze przygotowanymi rezerwami mobilizacyjnymi.

Przyjmuje się, że zadaniem armii zawodowej w czasie pokoju jest przede wszystkim zapobieżenie wybuchowi konfliktu. W razie wojny na dużą skalę działania muszą być prowadzone przez siły zbrojne rozwinięte mobilizacyjnie do stanu potrzebnego na ten czas. Rozwinięcie oraz powszechność obrony zapewniają systematycznie przeszkalane rezerwy mobilizacyjne, wraz

z utrzymywaniem dla nich na czas rozwinięcia uzbrojeniem i sprzętem. Wobec współczesnych potrzeb jest to rozwiązanie adekwatne oraz racjonalne.

Na potrzeby szkolenia rezerw mobilizacyjnych należy maksymalnie wykorzystać wzmoczoną aktywność wszelkich pozarządowych organizacji społecznych o charakterze proobronnym. Dobrym krokiem w tym kierunku jest zorganizowanie się części organizacji, przy wsparciu Ministerstwa Obrony Narodowej, w krajową federację takich podmiotów.

Ważnym elementem systemu rezerw wojskowych powinny stać się także zreformowane Narodowe Siły Rezerwowe. Reformując je należy przejść od pojedynczych etatów NSR ulokowanych dziś w wojskach operacyjnych do ustanowienia odrębnych, podporządkowanych terytorialnie, formacji (oddziałów) NSR, stanowiących pierwszy, „elitarny” i operacyjny (w odróżnieniu od rezerw mobilizacyjnych) rzut strategicznych rezerw Sił Zbrojnych RP.

Główne zadania operacyjne tak zreformowanych NSR powinny obejmować lokalne wsparcie działania wojsk operacyjnych i innych służb państwa w zapewnianiu bezpieczeństwa terytorialnego czy też udział w działaniach nieregularnych na terytorium opanowanym przez przeciwnika.

6. Wdrożenie „trzeciej fali” modernizacji technicznej Sił Zbrojnych RP – cyberobrona, systemy bezzałogowe, broń precyzyjnego rażenia

Zadanie: konsekwentnie realizować wieloletni program modernizacji technicznej SZ RP zgodnie z przyjętymi priorytetami oraz przygotować program „trzeciej fali” modernizacyjnej ukierunkowany na szeroką informatyzację wojska (cyberobrona, bezzałogowce, broń precyzyjnego rażenia, w tym oparta na wykorzystaniu technologii satelitarnych).

Siły Zbrojne stanowią syntezę trzech czynników: człowieka, broni oraz organizacji. Najważniejszy jest kapitał osobowy. Ważne są także rozwiązania organizacyjne. Jednak kwintesencją armii jest broń. Bez niej nawet największa i najlepiej zorganizowana grupa ludzi nie byłaby pełnowartościową armią. Dlatego rozwój uzbrojenia i technologii wojskowych oraz ciągła modernizacja techniczna jest czynnikiem, który w głównej mierze przesądza o sile i obliczu sił zbrojnych oraz determinuje kierunki transformacji wojska.

Przeprowadzany w sposób racjonalny, planowy i długoterminowy rozwój Sił Zbrojnych ma w Polsce blisko piętnastoletnią historię. Jej początkiem było ustanowienie w 2001 r. ustawowego, stałego wskaźnika nakładów budżetowych na wojsko na poziomie nie niższym niż 1,95 proc. PKB (oraz dodatkowo, w odrębnej ustawie, 0,05 proc. PKB na wieloletni program sfinansowania zakupu samolotu wielozadaniowego).

W ramach planowej modernizacji do dziś w Siłach Zbrojnych zrealizowano kilka ważnych programów, które można określić jako „pierwszą falę” modernizacji Wojska Polskiego w XXI w. Dotyczyła ona przede wszystkim pozyskania samolotu wielozadaniowego F-16, kołowego transportera opancerzonego ROSOMAK czy przeciwpancernego systemu raketowego SPIKE.

Obecnie realizowana jest „druga fala” modernizacyjna. Składają się na nią programy uruchamiane zgodnie z priorytetami ustanowionymi w rządowo-prezydenckich Głównych Kierunkach Rozwoju Sił Zbrojnych RP oraz ich Przygotowań do Obrony Państwa na lata 2013–2022:

- obrona powietrzna, w tym przeciwraketowa;
- systemy informacyjne (łączość, rozpoznanie, dowodzenie);
- mobilność wojsk lądowych, zwłaszcza śmigłowcowa.

Zrealizowanie tych programów pozwoli zaliczyć Siły Zbrojne RP do głównego trzonu sił NATO. Istotnym wsparciem będzie tu podniesienie stałego wskaźnika nakładów budżetowych na obronność do poziomu co najmniej 2 proc. PKB.

Natomiast w najbliższej przyszłości polskie Siły Zbrojne czeka realizacja priorytetów w ramach „trzeciej fali” modernizacyjnej, której założenia zostaną nakreślone w przygotowywanych Głównych Kierunkach Rozwoju Sił Zbrojnych RP oraz ich Przygotowań do Obrony Państwa na lata 2017–2026.

Analogicznie do tofflerowskiej teorii rozwoju cywilizacyjnego, „trzecia fala” modernizacyjna Wojska Polskiego w XXI w. będzie technologicznym skokiem w sferze informacyjnej. Oznacza to masowe wyposażenie Sił Zbrojnych RP w z informatyzowane systemy walki i wsparcia. Proces ten powinien zakończyć się w trzeciej lub czwartej dekadzie XXI w.

W ramach „trzeciej fali” priorytetowo potraktowane muszą być następujące trzy modernizacyjne programy rozwoju Sił Zbrojnych RP:

- Środki cyberobrony (szerzej – cyberwalki, cyberbroni) – walka o panowanie w cyberprzestrzeni będzie jeszcze istotniejszym warunkiem powodzenia, niż np. znana w ostatnim wieku walka o panowanie w powietrzu.
- Bezzałogowe systemy walki i wsparcia – rewolucja informacyjna pozwala i wręcz wymusza coraz szersze zastępowanie człowieka przez wysoce z informatyzowane systemy bezzałogowe (drony). Tak jak w XX w. kawaleria została wyparta przez czołgi, tak w XXI w. maszyny załogowe zostaną wyparte przez maszyny bezzałogowe.
- Broń precyzyjnego rażenia, w tym wykorzystująca satelitarne technologie bezpieczeństwa, tj. systemy wykorzystania przestrzeni kosmicznej dla potrzeb bezpieczeństwa państwa, w tym sił zbrojnych (jak wszelkie inne z informatyzowane systemy walki i wsparcia, systemy bazujące np. na operowaniu w cyberprzestrzeni nie mogą skutecznie działać bez jednoczesnego wykorzystania przestrzeni kosmicznej). Łączność satelitarna, wykorzystanie satelitów do rozpoznania, monitorowania, kierowania, dowodzenia itp., to podstawowy warunek skutecznego funkcjonowania z informatyzowanych sił zbrojnych, nasyconych technologiami informatycznymi.

7. Uruchomienie i realizacja Narodowego Programu Systemów Bezzałogowych (koło zamachowe innowacyjności dla bezpieczeństwa i rozwoju)

Zadanie: uruchomić i zrealizować Narodowy Program Systemów Bezzałogowych jako motor innowacyjności dla bezpieczeństwa i rozwoju gospodarczego, zwłaszcza innowacyjności polskiego przemysłu obronnego.

Polska stoi przed szansą znalezienia się w czołówce międzynarodowych producentów systemów bezzałogowych. Ten innowacyjny kierunek stwarza także unikatową szansę skoku generacyjnego dla polskiego potencjału badawczo-produkcyjnego w sferze obronności.

Systemy bezzałogowe należą do najbardziej perspektywicznych systemów służących bezpieczeństwu, w tym systemów obronnych i ochronnych. Znajdują one także zastosowanie w pozostałych gałęziach gospodarki oraz wielu sferach życia publicznego i prywatnego. Za wykorzystaniem bezzałogowców przemawia ich skuteczność, wydajność, a także względy ekonomiczne i – co najważniejsze – zmniejszenie ryzyka utraty życia lub zdrowia przez ludzi.

Dlatego też ich wykorzystywanie oraz rozwój musi stać się jednym z priorytetów modernizacyjnych, co już dzieje się m.in. w polskiej armii. W przyszłości ich wykorzystanie, także przez publiczne i niepubliczne służby oraz straże ochronne, odbywać się będzie na jeszcze większą skalę. Czekają nas ponadto wzrost komercyjnego zapotrzebowania na bezzałogowce, ponieważ grono użytkowników takich systemów, a także liczba ich zastosowań stale się powiększa.

Przy wykorzystaniu bezzałogowców w obszarze bezpieczeństwa kluczową sprawą są informatyczne systemy kierowania i zarządzania nimi, czyli „panowanie kryptograficzne” (własne kody źródłowe oprogramowania), bez którego nie można w pełni polegać na używanym wyposażeniu. To jeden z najważniejszych argumentów za ustanowieniem własnego, narodowego programu ich rozwoju i produkcji.

Aby w pełni władać bezzałogowcami na poziomie operacyjnym, muszą być one polskiej produkcji. Zakupy zagraniczne są w takiej sytuacji obciążone zbyt dużym ryzykiem, aby opierać na nich wyposażanie polskich sił i struktur bezpieczeństwa narodowego.

Polska nauka i przemysł dysponują obiecującym potencjałem kadrowym oraz technicznym, stwarzającym szanse dla innowacyjności, aby w perspektywie dekady projektować i produkować pełną gamę bezzałogowców różnych klas i typów.

Wykorzystując tę szansę Polska może znaleźć się w europejskiej czołówce państw-producentów bezzałogowców, a także współpracować z międzynarodowymi producentami, np. w ramach europejskiego programu bezzałogowców.

Niezbędne dla uruchomienia inicjatywy Narodowego Programu Systemów Bezzałogowych jest zainteresowanie oraz współdziałanie trzech grup: użytkowników, określających potrzeby (Siły Zbrojne RP, Policja, służby, straże); potencjału naukowego skupionego na projektowaniu narodowych rozwiązań (w tym Narodowe Centrum Badań i Rozwoju); potencjału produkcyjnego realizującego określone projekty (podmioty polskiego przemysłu obronnego). Współpraca powyższych środowisk oraz uzyskanie efektu synergii, stanowi podstawowy sposób realizacji tego złożonego wyzwania. Stworzy także unikatową szansę skoku generacyjnego polskiego potencjału badawczo-rozwojowego i produkcyjnego w sferze obronności, czyniąc bezzałogowce wizytówką narodowego potencjału obronnego.

8. Działania wzmacniające Sojusz Północnoatlantycki

Zadanie: rozwinąć na forum międzynarodowym działania wzmacniające mechanizmy obrony kolektywnej NATO, w tym potencjał obronny na wschodniej flance Sojuszu, zwłaszcza przez przekształcanie rotacyjnej obecności sił zbrojnych państw sojuszniczych w regionie w stałą.

NATO adekwatnie zareagowało na wybuch konfliktu na wschodzie. Zwiększono sojuszniczą aktywność i obecność wojskową na terenie państw flankowych, a także na Morzu Bałtyckim i Morzu Czarnym.

Jednak wobec trwałości spowodowanych przez Rosję zmian w środowisku bezpieczeństwa, ważną kwestią stała się trwała strategiczna adaptacja polityki Sojuszu, szczególnie poprzez wzmocnienie mechanizmów obrony kolektywnej.

Istotne kierunki tej adaptacji – prowadzące do strategicznego wzmocnienia potencjału na wschodniej flance NATO – przyjęte zostały na szczycie Sojuszu w Newport w 2014 r. Najważniejsze z nich to ciągła, rotacyjna obecność wojskowa na wschodniej flance, połączona ze zwiększoną aktywnością ćwiczeniową; utworzenie tzw. „szpicy”, czyli sił natychmiastowego

reagowania (VJTF); utworzenie wysuniętych elementów dowódczych z niezbędną infrastrukturą logistyczną i wsparciem; konkretyzacja planów ewentualnościowych z możliwym przekształceniem w przyszłości niektórych z nich w stałe plany obrony.

Na szczycie NATO w Warszawie (zaplanowanym na 8–9 lipca 2016 r.) należy podsumować realizację tych zadań. Jednocześnie ważne będzie, aby zaprojektować kierunki dalszej strategicznej adaptacji Sojuszu.

W tym zakresie najważniejsze powinno być zbudowanie zdolności do odstraszenia, powstrzymania, zniechęcania potencjalnego przeciwnika przed agresją poniżej progu otwartej, regularnej wojny. Sojusz ma niewątpliwie wiarygodny potencjał odstraszenia, włącznie z odstraszeniem nuklearnym, przed wielkoskalową agresją na swoje terytorium. Natomiast trudności z reagowaniem i uzyskaniem konsensusu wewnątrz NATO mogą wystąpić w razie agresji nieregularnej, asymetrycznej, agresji hybrydowej o niskiej intensywności, w tym zwłaszcza agresji poniżej progu otwartej wojny.

Jednym z ważnych sposobów zniechęcania potencjalnego agresora przed takim działaniem jest zapewnienie stałej obecności na terytorium państw brzegowych NATO wojsk z innych państw sojuszniczych. Potencjalny agresor musiałby wówczas w kalkulować w swój strategiczny rachunek wejście w konflikt nie tylko z krajem będącym celem agresji, ale także krajami, których wojska byłyby rozmieszczone na terytorium zaatakowanego państwa.

Dlatego konieczne jest umacnianie obecności wojskowej w krajach brzegowych, w tym w szczególności nadawanie jej coraz bardziej stałego charakteru. Przyjętą w Newport koncepcję „szpicy” oraz system ćwiczebnej obecności rotacyjnej należałoby uzupełnić na szczycie w Warszawie „czatą”, czyli stałą obecnością nawet niezbyt liczebnych, ale wyraźnie widocznych sił sojuszniczych i odpowiedniej infrastruktury w strefie nadgranicznej NATO.

Ważne jest także, aby doktryna użycia „szpicy”, czyli sił natychmiastowego reagowania (VJTF), zakładała ich uprzedzające rozwinięcie na kierunku zagrożenia już w fazie narastania kryzysu, a nie dopiero w formie reakcji na zaistniałą już agresję. Do wzmocnienia szybkości działania VJTF przyczyni się także uprzednie rozlokowanie sprzętu i uzbrojenia wojskowego w państwach brzegowych („*prepositioning*”).

Wydaje się także, że w obliczu skali, charakteru i przewidywanej trwałości zmian środowiska bezpieczeństwa, konieczna będzie też fundamentalna refleksja wewnątrz NATO, dotycząca nowelizacji Koncepcji Strategicznej przyjętej w Lizbonie w 2010 r. Warto, aby prace nad nią mogły być uruchomione już na najbliższym szczycie Sojuszu w Warszawie, z perspektywą przyjęcia nowej koncepcji na szczycie w 2018 r.

9. Działania prowadzące do strategicznego upodmiotowienia Unii Europejskiej i rozwoju współpracy NATO-UE (polityczno-strategiczna odpowiedź na zagrożenia hybrydowe)

Zadanie: kontynuować starania o uzgodnienie nowej, wspólnej i realnej strategii bezpieczeństwa UE, przy uwzględnieniu jej komplementarności z NATO oraz rozwinięcia systemowych mechanizmów współdziałania NATO-UE (budowa euroatlantyckiego „tandemu bezpieczeństwa”).

Unia Europejska jest jednym z filarów bezpieczeństwa RP. Mimo że NATO pozostaje głównym międzynarodowym gwarantem bezpieczeństwa militarnego, w tym Polski i innych państw Europy Środkowej, reakcja na konflikt rosyjsko-ukraiński pokazała, że Unia dysponuje dużym potencjałem odstraszenia, realizowanego za pomocą instrumentów ekonomicznych, takich jak sankcje gospodarcze.

Unia może także uzupełniać kompetencje Sojuszu w zakresie bezpieczeństwa pozamilitarnego, w tym bezpieczeństwa energetycznego, cybernetycznego, finansowego i społecznego.

Jednak, aby potencjał Unii Europejskiej, jako filaru bezpieczeństwa RP, został w pełni wykorzystany, musi ona stać się istotnym podmiotem strategicznym w dziedzinie bezpieczeństwa i obrony. Dlatego też Polska dąży do wzmacniania unijnej Wspólnej Polityki Bezpieczeństwa i Obrony (WPBiO), angażując się w rozwój tej inicjatywy i definiowanie jej przyszłego kształtu.

Głównym wyzwaniem Wspólnej Polityki Bezpieczeństwa i Obrony UE – co uwidocznili obecny kryzys na Ukrainie – jest brak jednolitej strategii, z którą utożsamiałyby się wszystkie państwa członkowskie. Unia Europejska potrzebuje strategii, aby stać się bardziej sprawną i skuteczną instytucją. Strategia ta powinna odnosić się do spraw wojskowych, ale też (a może przede wszystkim) do pozamilitarnych aspektów bezpieczeństwa.

Potrzebne są działania budujące poczucie podmiotowości Unii Europejskiej, jako strategicznego aktora bezpieczeństwa, szczególnie w obliczu dynamicznie zmieniającego się środowiska bezpieczeństwa, na jej wschodniej flance. Kluczowa dla wzmocnienia podmiotowości UE będzie realizacja zadania postawionego na szczycie Rady Europejskiej 25–26 czerwca 2015 r., zlecającego opracowanie do czerwca 2016 r. unijnej Globalnej Strategii Polityki Zagranicznej i Bezpieczeństwa.

Szczególnie ważna jest także współpraca na forum NATO-UE. Wydaje się, że obecnie jest właściwy moment na przełamanie wieloletniego impasu oraz podjęcie działań zmierzających do budowy euroatlantyckiego tandemu bezpieczeństwa.

Jest to istotne w obliczu współczesnej złożoności zagrożeń bezpieczeństwa w Europie, hybrydowości oznaczającej jednoczesne stosowanie zróżnicowanych metod i środków presji oraz agresji: od politycznych, dyplomatycznych, informacyjnych, poprzez ekonomiczne, finansowe, energetyczne, cybernetyczne, aż do militarnych we wszelkich możliwych stopniach ich nasilenia (w tym agresji poniżej progu otwartej, regularnej wojny, szczególnie niebezpiecznej dla sojusznicznych/wspólnotowych organizacji).

W przeciwstawianiu się zagrożeniom hybrydowym tandem UE-NATO to optymalne rozwiązanie. UE byłaby szczególnie skuteczna w pozamilitarnej sferze bezpieczeństwa, NATO w polityczno-militarnej.

10. Umocnienie strategicznych partnerstw, szczególnie sojuszu z USA

Zadanie: zabiegać o stałe stacjonowanie amerykańskich wojsk w Polsce i regionie (m.in. systemów obrony przeciwrakietowej, sił powietrznych, wojsk specjalnych) oraz rozszerzać polsko-amerykańską współpracę polityczno-wojskową również o wymiary pozamilitarne. Jednocześnie zacieśniać relację z kluczowymi sojusznikami europejskimi oraz z państwami regionu leżącymi na wschodniej flance NATO.

Strategiczne partnerstwo ze Stanami Zjednoczonymi jest trzecim – obok członkostwa w NATO i Unii Europejskiej – zewnętrznym filarem bezpieczeństwa RP. W interesie Polski leży też zabieganie o trwałość i jakość więzi transatlantyckich, bazujących na fundamencie wojskowej obecności USA w Europie, szczególnie na wschodniej flance NATO.

Od momentu wybuchu konfliktu rosyjsko-ukraińskiego Stany Zjednoczone podjęły szereg działań wzmacniających bezpieczeństwo Europy Środkowo-Wschodniej, także w ramach Inicjatywy Wzmocnienia Bezpieczeństwa Europejskiego (*European Reassurance Initiative*), ogłoszonej przez prezydenta USA Baracka Obamę w Warszawie w dniu Święta Wolności 4 czerwca 2014 r.

Polegają one m.in. na ciągłej, rotacyjnej obecności amerykańskich sił w regionie czy ostatecznych decyzjach o rozmieszczeniu w Polsce, państwach bałtyckich oraz Rumunii i Bułgarii uzbrojenia i sprzętu militarnego dla amerykańskich wojsk. Należy dążyć, aby działania te nabierały coraz bardziej trwałego charakteru i w perspektywie tworzyły odpowiednie warunki do stałego stacjonowania amerykańskich wojsk na terytorium RP.

Obecnie priorytetowego znaczenia dla polsko-amerykańskiego partnerstwa strategicznego nabiera planowy rozwój sojuszniczego systemu obrony przeciwrakietowej, którego kluczowy element stanowi amerykański komponent w ramach EPAA (*European Phased Adaptive Approach*). W jego skład od 2018 r. ma wejść baza obrony przeciwrakietowej zlokalizowana w Redzikowie, której budowa powinna rozpocząć się w przyszłym roku. Istotnym elementem wzmocnienia współpracy powinna być też kontynuacja kooperacji techniczno-wojskowej.

Poza współpracą w zakresie „twardego” bezpieczeństwa Polska powinna dążyć do rozszerzenia dwustronnego dialogu strategicznego ze Stanami Zjednoczonymi w dziedzinie bezpieczeństwa o kwestie związane ze wsparciem demokracji na świecie, zagrożeniami cybernetycznymi, bezpieczeństwem energetycznym oraz kooperacją naukowo-techniczną. Szczególnego znaczenia nabiera perspektywa współpracy w dziedzinie energetyki.

Wzmocnieniu współpracy ze Stanami Zjednoczonymi powinien towarzyszyć rozwój i umacnianie regionalnych i bilateralnych partnerstw Polski z najważniejszymi europejskimi sojusznikami (Trójkąt Weimarski, Wielka Brytania), jak również z państwami wschodniej flanki (Grupa Wyszehradzka, państwa bałtyckie, Rumunia, Bułgaria), a także z państwami skandynawskimi. Szczególnie obiecujące wydają się inwestycje w format państw wschodniej flanki, co może przynieść wymierne korzyści zarówno w zakresie działań bilateralnych, jak także w ramach NATO i Unii Europejskiej.
