BIURO BEZPIECZEŃSTWA NARODOWEGO

WYBRANE DOKUMENTY ORAZ OPRACOWANIA WYDANE PRZEZ BIURO BEZPIECZEŃSTWA NARODOWEGO W LATACH 2010-2015

WARSZAWA 2015

Publikacja zawiera wybrane dokumenty oraz inne opracowania przygotowane przez Biuro Bezpieczeństwa Narodowego w czasie kadencji Prezydenta Rzeczypospolitej Polskiej Bronisława Komorowskiego w latach 2010-2015

Materiały zostały opacowane przez analityków BBN, także w ramach współpracy z niezależnymi środowiskami eksperckimi.

Publikacja zawiera również dwa dokumenty – Strategia Bezpieczeństwa Narodowego RP oraz uzasadnienie do projektu ustawy wprowadzającej reformę systemu kierowania i dowodzenia Siłami Zbrojnymi RP – które powstały przy ścisłej współpracy z Biurem Bezpieczeństwa Narodowego.

W opracowaniu, ze względu rozmiar, pominięta został wydana w 2013 r. Biała Księga Bezpieczeństwa Narodowego RP, będąca jedną z najważniejszych publikacji w historii BBN. Dostępna jest ona w głównych bibliotekach w całej Polsce, a także na stronie internetowej www.spbn.gov.pl.

SPIS DOKUMENTÓW

PROJEKT DOKTRYNY BEZPIECZEŃSTWA INFORMACYJNEGO RP

Prace nad dokumentem, przygotowywanym na polecenie Prezydenta RP Bronisława Komorowskiego, związane były z eskalacją zagrożeń hybrydowych – w tym o charakterze informacyjnym – jak propaganda, dezinformacja czy psychologiczne zastraszanie ze strony obcych państw i aktorów niepaństwowych (np. organizacji terrorystycznych). Problem ten był m.in. tematem posiedzenia Rady Bezpieczeństwa Narodowego, jakie odbyło się 18 lutego 2015 r.

Prace nad dokumentem zostały rozpoczęte na początku 2015 r. i były prowadzone we współpracy z przedstawicielami służb oraz właściwych instytucji państwa, uczelni oraz pozarządowych ośrodków analitycznych.

Projekt został opublikowany 24 lipca 2015 r. Jednocześnie należy zaznaczyć, że prace nad Doktryną powinny być kontynuowane.

Rekomendacje i oceny zawarte w Doktrynie – mającej być dokumentem wykonawczym do Strategii Bezpieczeństwa Narodowego RP – powinny stać się podstawą do koordynacji działań państwa, sektora prywatnego i obywateli wobec zagrożeń informacyjnych.

BIURO BEZPIECZEŃSTWA NARODOWEGO

24 lipca 2015 r.

PROJEKT DOKTRYNY BEZPIECZEŃSTWA INFORMACYJNEGO RP

WPROWADZENIE

1. Bezpieczeństwo informacyjne – wraz z jego integralną częścią, jaką jest cyberbezpieczeństwo - jest jednym z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, mającym charakter transsektorowy i wpływającym na efektywność funkcjonowania całego systemu bezpieczeństwa.
2. Działania na rzecz bezpieczeństwa informacyjnego muszą być podejmowane z uwzględnieniem ochrony praw człowieka i obywatela, a szczególnie poszanowaniem prawa do wolności słowa oraz prywatności. Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnej i wiarygodnej analizie ryzyka.
3. Punktem wyjścia niniejszej Doktryny są kierunkowe postanowienia Strategii Bezpieczeństwa Narodowego RP dotyczące bezpieczeństwa informacyjnego i ochrony informacji niejawnych oraz cyberbezpieczeństwa. Ten ostatni wymiar bezpieczeństwa informacyjnego został już wcześniej rozwinięty w przyjętej w 2015 r. Doktrynie cyberbezpieczeństwa RP i w niniejszym dokumencie nie będzie szerzej podejmowany. W przyszłości należałoby scalić obydwa dokumenty w jeden.
4. Główne pojęcia przyjęte w Doktrynie bezpieczeństwa informacyjnego RP:
   - **Bezpieczeństwo informacyjne państwa -** transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Osiąga się to poprzez realizacje takich zadań jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa informacyjnego (operacyjnej i preparacyjnej), a do ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego.
   - **Środowisko bezpieczeństwa informacyjnego** (przestrzeń informacyjna, infosfera) – zewnętrzne i wewnętrzne, militarne i niemilitarne (cywilne), osobowe, technologiczne i organizacyjne warunki bezpieczeństwa (warunki realizacji interesów danego podmiotu w dziedzinie bezpieczeństwa informacyjnego i osiągania ustalonych przezeń

celów w tym zakresie), charakteryzowane przy pomocy takich kategorii, jak zagrożenia, wyzwania oraz szanse i ryzyka:

  - **zagrożenia bezpieczeństwa informacyjnego** – pośrednie lub bezpośrednie, zakłócające lub destrukcyjne oddziaływania na podmiot;
  - **wyzwania bezpieczeństwa informacyjnego** – sytuacje problemowe w obszarze bezpieczeństwa informacyjnego, stwarzane zwłaszcza przez szanse i ryzyka oraz generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw w tym zakresie;
  - **szanse bezpieczeństwa informacyjnego** – niezależne od woli podmiotu okoliczności (zjawiska i procesy w środowisku bezpieczeństwa informacyjnego) sprzyjające realizacji interesów oraz osiąganiu celów podmiotu w obszarze bezpieczeństwa informacyjnego;
  - **ryzyka bezpieczeństwa informacyjnego** – niebezpieczne dla funkcjonowania w przestrzeni informacyjnej konsekwencje przyszłych własnych działań.

- **Komunikacja strategiczna –** synteza działań informacyjnych danego podmiotu strategicznego (np. państwa, sojuszu, koalicji) ukierunkowanych na kształtowanie poglądów, ocen, opinii itp. oraz decyzji innych podmiotów z otoczenia strategicznego (podległych, współdziałających, neutralnych, konkurujących, wrogich) w sposób korzystny dla własnych interesów strategicznych. Realizowana jest poprzez aktywność w takich obszarach, jak: dyplomacja publiczna, komunikacja społeczna, operacje informacyjne oraz operacje psychologiczne.
- **Dyplomacja publiczna** – część dyplomacji danego państwa realizowana w publicznej przestrzeni informacyjnej jako forma pozytywnego wpływania na postawy społeczne w innych krajach i kształtowania w ten sposób polityki zagranicznej danego państwa. Cechą szczególną dyplomacji publicznej jest wykorzystywanie środków wykraczających poza zakres tradycyjnie pojmowanej dyplomacji, a jej istotnym elementem jest kształtowanie opinii publicznej w innych krajach przy pomocy mechanizmów wykorzystywanych przez marketing gospodarczy oraz polityczny.
- **Komunikacja społeczna** proces wytwarzania, przekształcania i przekazywania informacji między jednostkami, grupami i organizacjami społecznymi, mający na celu dynamiczne kształtowanie, modyfikację bądź zmianę wiedzy, postaw i zachowań w kierunku zgodnym z wartościami i interesami oddziałujących na nie podmiotów. W komunikacji społecznej nadawca w przekazie może wykorzystywać środki perswazji lub manipulacji medialnej w celu wywołania określonego zachowania u odbiorcy.
- **Operacje informacyjne (walka informacyjna)** czynności polegające na oddziaływaniu na informacje i/lub systemy informacyjne w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika (zautomatyzowanych oraz z udziałem czynnika ludzkiego), przy jednoczesnej ochronie własnych procesów decyzyjnych; w wymiarze wojskowym także działalność mająca na celu wywarcie pożądanego wpływu na wolę, rozumienie i zdolności przeciwników, potencjalnych przeciwników lub innych stron konfliktu, wspierających cele danej misji; w operacjach informacyjnych można wyróżnić działania ofensywne i defensywne:
- **do działań ofensywnych** należy zaliczyć: operacje psychologiczne, pozorację, destrukcję, walkę elektroniczną, atak informatyczny, działania z zakresu komunikacji społecznej;
- **do działań defensywnych** należy zaliczyć: bezpieczeństwo informacyjne, osłonę, działania kontrpropagandowe, działania kontrwywiadowcze, walkę elektroniczną, informacyjne działania specjalne.
- **Operacje psychologiczne** – operacje mające na celu wpływanie na emocje, motywacje, obiektywne rozumowanie, a ostatecznie zachowanie rządów państw obcych,

organizacji, grup i osób będących celami tych operacji, tak aby osiągnąć efekt w postaci wzmocnienia lub nakłonienia do zachowań korzystnych dla realizacji własnych interesów. Mogą być wykorzystywane zarówno w czasie pokoju (klęsk żywiołowych, stanów kryzysowych i alarmowych), jak i podczas wojny.

- **Inżynieria społeczna** – zespół metod i środków celowego manipulowania społeczeństwem.
- **Propaganda, dezinformacja –** rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich), w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego, lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń.
- **Manipulacja informacją –** wykorzystanie prawdziwych informacji, ale w taki sposób, żeby wywołać fałszywe implikacje, np. drogą pomijania niektórych, istotnych, ale niewygodnych informacji lub poprzez taki dobór informacji, żeby budziły fałszywe skojarzenia.
- **Trollowanie** (trolling) – antyspołeczne zachowanie charakterystyczne dla internetowych grup, forów dyskusyjnych, czatów i sieci społecznościowych, polegające na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych przekazów.

1. CELE STRATEGICZNE RP W DZIEDZINIE BEZPIECZEŃSTWA INFORMACYJNEGO

1. Interesem narodowym w obszarze bezpieczeństwa informacyjnego jest dysponowanie skutecznym narodowym potencjałem bezpieczeństwa zapewniającym gotowość i zdolność do zapobiegania zagrożeniom występującym w przestrzeni informacyjnej (infosferze, infoprzestrzeni), w tym odstraszania, obrony i ochrony przed nimi oraz likwidowania ich następstw.
2. 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.
3. Cele strategiczne osiąga się poprzez realizację zadań prowadzących do osiągania celów o charakterze operacyjnym i preparacyjnym. Głównym celem operacyjnym jest panowanie we własnej przestrzeni informacyjnej (infosferze) oraz selektywna obrona interesów narodowych w zewnętrznej (obcej) przestrzeni informacyjnej (infosferze). Osiąga się go poprzez realizacje takich zadań, jak:
   - utrzymywanie i demonstrowanie gotowości do przeciwdziałania zagrożeniom informacyjnym;
   - rozpoznanie, analiza i ocena zagrożenia informacyjnego;
   - ochrona strategicznych zasobów informacyjnych państwa;
   - reagowanie na zagrożenia i podejmowanie działań ofensywnych w zakresie walki informacyjnej;
   - kształtowanie świadomości społecznej w zakresie celów polityki informacyjnej państwa oraz interesu narodowego;
   - bieżące rozpoznanie systemu wartości oraz słabych stron przeciwnika.

4. Do osiągnięcia celów operacyjnych niezbędne jest, w wymiarze preparacyjnym, zbudowanie, utrzymywanie i systematyczne doskonalenie (rozwój) zintegrowanego, zarządzanego (koordynowanego) ponadresortowo, systemu bezpieczeństwa informacyjnego RP obejmującego:
   - podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie bezpieczeństwa informacyjnego;
   - podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia działań defensywnych (ochronnych i obronnych) oraz ofensywnych w zakresie bezpieczeństwa informacyjnego i walki informacyjnej, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych.

2. ŚRODOWISKO BEZPIECZEŃSTWA INFORMACYJNEGO RP

2.1. WYMIAR WEWNĘTRZNY

2.1.1. Zagrożenia

5. Zagrożeniem płynącym z funkcjonowania w środowisku informacyjnym może być rozpowszechnianie i powielanie treści propagandowych mające na celu ukazanie polskiej racji stanu w negatywnym świetle, co *de facto* szkodzi interesowi państwa (stosowanie prowokacji, celowe manipulowanie przekazem poprzez wyrywanie z kontekstu fragmentów wypowiedzi polityków RP, nadawanie im kontrowersyjnego charakteru).
6. Do najpoważniejszych zagrożeń związanych z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego należy zaliczyć:
   - występowanie w społeczeństwie deficytów informacyjnych, skutkujących podatnością na wrogą perswazję;
   - potencjalna dezinformacja obywateli poprzez agresywne działania propagandowe; dywersja ideologiczna – narzucanie obcych idei niezgodnych z interesem państwa;
   - pojawienie się i rozwój postaw antypaństwowych; nasilenie się postaw agresywnych, defetystycznych (np. islamofobia, szpiegomania);
   - wzrost negatywnych postaw społecznych lub wystąpienie konfliktów społecznych, zgodnych z intencjami przeciwnika informacyjnego (informacyjnego napastnika);
   - istnienie (tworzenie) agentury wpływu (inspirowanie do zakładania oraz wsparcie finansowe formacji politycznych lub organizacji społecznych wspierających i realizujących obce interesy w Polsce);
   - wpływanie na opinię publiczną przez agentów zmiany sterowanych z zewnątrz, zwłaszcza aktywizacja wybranych grup społecznych przez inne państwo oraz realizacja interesów obcych państw, sprzecznych z interesem RP;
   - obniżanie się morale społeczeństwa w razie agresji informacyjno-propagandowej, rzutujące negatywnie na polityczno-militarne procesy decyzyjne.
7. Do zagrożeń informacyjnych związanych z funkcjonowaniem w cyberprzestrzeni należą:
   - dezinformacja, trolling, wroga propaganda, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego;
   - ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną;

- istnienie technologicznych luk, które dają szansę, także niezauważonej, ingerencji w treści portali internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni.

8. Odrębnym obszarem występowania potencjalnych zagrożeń jest przestrzeń medialna:
   - monopolizacja rynku informacyjnego i jego poszczególnych struktur oraz niekontrolowany rozwój rynku informacyjnego media masowe mogą być narzędziem dezinformacji;
   - przejmowanie lub finansowanie mediów przez podmioty nieprzychylne lub wrogie Polsce;
   - pojawienie się w przestrzeni informacyjnej mediów propagujących idee sprzeczne z interesem narodowym;
   - aktywne uczestnictwo przeciwnika w polskich mediach społecznościowych – propagowanie idei sprzecznych z interesem narodowym;
   - nieświadome, niezamierzone powielanie przekazu informacyjnego sprzecznego z interesem narodowym przez użytkowników mediów społecznościowych lub media masowe.
9. Poważnym zagrożeniem może okazać się eksploatowanie drażliwych kwestii w kontaktach międzynarodowych, w tym bilateralnych, przy wykorzystaniu wsparcia określonych podmiotów i osób.

2.1.2. Wyzwania (ryzyka i szanse)

10. Istotnym ryzykiem w obszarze bezpieczeństwa informacyjnego może być niewystarczająca adaptacja strukturalna i koordynacyjna działań w obliczu zagrożenia informacyjnego, szczególnie w kreowaniu spójnej polityki informacyjnej oraz działań w zakresie bezpieczeństwa informacyjnego.
11. Ryzyka systemowe (odnoszące się do niedoskonałego funkcjonowania podsystemu bezpieczeństwa informacyjnego państwa):
    - brak właściwej ochrony własnych militarnych systemów informacyjnych i ocen słabości systemów informacyjnych potencjalnych przeciwników;
    - brak efektywnego systemu kształcenia i szkolenia w zakresie bezpieczeństwa informacyjnego;
    - niewystarczająca liczba wykwalifikowanych pracowników bezpieczeństwa informacyjnego;
    - brak jednolitego, skoordynowanego przekazu informacyjnego ze strony struktur rządowych formułowanego do społeczeństwa;
    - brak systemu finansowania przedsięwzięć na rzecz zapewnienia bezpieczeństwa informacyjnego;
    - niska reaktywność systemowa wobec agresji informacyjno-propagandowej;
    - nieadekwatne do zagrożeń wzorce doktrynalne.
12. Ryzykiem w dziedzinie bezpieczeństwa informacyjnego może być podejmowanie przez organy państwa decyzji na podstawie informacji niepełnych, niesprawdzonych lub dezinformacji.
13. Źródłem ryzyk może okazać się również dysonans informacyjny różnych ośrodków informacyjnych.

14. Naruszenia praw i wolności obywateli w zakresie prawa do prywatności.
15. Szansę stanowić może potencjał społeczeństwa obywatelskiego, który można wykorzystać na rzecz zwiększenia bezpieczeństwa informacyjnego.
16. Wykorzystanie potencjału informacyjnego państwa w ramach systemu bezpieczeństwa narodowego stanowi szansę na zwiększenie efektywności działań w obszarze bezpieczeństwa informacyjnego.
17. Zdobywanie wiedzy o naturze i skutkach zagrożeń informacyjnych dla funkcjonowania państwa może stanowić szansę na efektywne dostosowanie wykorzystywanych sił i środków.
18. Do szans zaliczyć należy także rozwój potencjału naukowego oraz wzrost konkurencyjności ośrodków informacyjnych.

2.2. WYMIAR ZEWNĘTRZNY

2.2.1. Zagrożenia

19. Wśród podstawowych zagrożeń w obszarze bezpieczeństwa informacyjnego państwa należy wskazać takie jak:
    - deformowanie treści oraz wprowadzanie do systemów informacyjnych nieprawdziwych treści logicznych za pośrednictwem kanałów łączności rządowej czy wojskowych systemów dowodzenia;
    - działalność służb specjalnych i podmiotów informacyjnych innych państw oraz aktorów niepaństwowych (w tym szpiegostwo);
    - wroga aktywność operacyjna struktur informacyjno-propagandowych aktorów państwowych i pozapaństwowych;
    - działania propagandowe i dezinformacyjne;
    - dominacja potencjalnych agresorów w środowisku informacyjnym;
    - penetracja środowiska informacyjnego RP przez wrogie struktury informacyjno-propagandowe;
    - utrata zdolności wpływania, dystrybucji informacji w środowisku informacyjnym.
20. Poważnym zagrożeniem są niepożądane, zewnętrzne oddziaływania informacyjne, mogące dotyczyć procedur sterowania procesami decyzyjnymi państwa, na które ukierunkowany jest atak informacyjny.
21. Skutkować to może bezpośrednim przełożeniem na koncepcje doktrynalne odnoszące się do infrastruktury wojskowej, systemów kierowania państwem i dowodzenia siłami zbrojnymi, a także szeroko rozumianych operacji informacyjnych.
22. Wśród najpoważniejszych zagrożeń związanych z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego należy zaliczyć:
    - inspirowane z zewnętrz działania informacyjne podmiotów wewnętrznych mające na celu wywoływanie i pogłębianie podziałów społecznych i politycznych;
    - wsparcie zewnętrzne dla podmiotów realizujących politykę przeciwnika;
    - dezinformacja obywateli innych państw, w tym tworzących wspólnoty organizacyjne w kwestiach dotyczących polskiej polityki zagranicznej.
23. Wśród istotnych zagrożeń związanych z funkcjonowaniem RP w wymiarze międzynarodowym wymienić należy:

- doprowadzenie do eskalacji napięć w stosunkach międzynarodowych, w tym bilateralnych i multilateralnych;
- kształtowanie negatywnego obrazu Polski na arenie międzynarodowej, w tym wśród sojuszników, przede wszystkim w ramach NATO i UE;
- wywoływanie w społeczeństwach i elitach politycznych tych państw nastrojów antypolskich na przykład poprzez nagłaśnianie i akcentowanie jednostkowych wypowiedzi przedstawicieli polityki, sprzecznych z oficjalną linią polityki zagranicznej RP w kluczowych, strategicznych sprawach;
- dyskredytowanie polskiej polityki zagranicznej na arenie międzynarodowej;
- działanie zagranicznych struktur informacyjnych przeciwko interesom RP;
- szerzenie treści antypolskich za pośrednictwem mediów o zasięgu międzynarodowym:
  - tworzenie w obiegu informacyjnym na Zachodzie obrazu Polski jako kraju ksenofobicznego i antysemickiego;
  - inspirowanie konfliktu polsko-litewskiego na tle mniejszości polskiej na Litwie – możliwość tworzenia przez wrogie służby specjalne wrażenia istnienia zbrojnego separatyzmu polskiego na Wileńszczyźnie;
  - inspirowanie konfliktu polsko-ukraińskiego na tle historycznym przy możliwym zastosowaniu zamachów terrorystycznych rzekomo dokonanych przez Ukraińców przeciw Polakom i odwrotnie;
- budowanie lobby interesów obcego państwa w ramach struktur wspólnotowych (UE, NATO).

24. W związku z funkcjonowaniem RP w globalnej cyberprzestrzeni mogą pojawić się zagrożenia w postaci ataków cybernetycznych na instytucje rządowe, pozarządowe i kulturalne kształtujące świadomość narodową lub blokady rządowego przekazu informacyjnego wskutek ataków cybernetycznych.

2.2.2. Wyzwania (ryzyka i szanse)

25. Ryzyko systemowe (odnoszące się do niedoskonałości funkcjonowania podsystemu bezpieczeństwa informacyjnego w skali międzynarodowej i krajowej) odnosi się do niskiej reaktywności i niewystarczającej koordynacji działań sojuszników RP w obliczu zagrożeń informacyjnych oraz potencjalnego wpływu niezrzeszonych państw na decyzje i kierunek polityki wspólnotowej i sojuszniczej.
26. Ryzyka mogą wypływać z niewłaściwego zarządzania sytuacjami kryzysowymi wynikającymi z szerzenia treści antypolskich za pośrednictwem mediów o zasięgu międzynarodowym:
  - konieczność walki z wizerunkiem „antysemickiej Polski”;
  - osłabienie pozycji Polski na arenie międzynarodowej, w tym w ramach NATO i UE, do izolacji włącznie;
  - dyskredytacja władz RP w celu obniżenia ich pozycji w stosunkach z przywódcami innych państw.
27. Szansą w zapewnieniu bezpieczeństwa informacyjnego może być rozwinięcie współpracy bilateralnej i regionalnej w kwestii zwalczania zagrożeń dla bezpieczeństwa informacyjnego:
  - nawiązanie ścisłej współpracy z odpowiednimi instytucjami ukraińskimi, wpływanie na ich kształt i kierunki działania;

- nawiązanie ścisłej współpracy z odpowiednimi instytucjami litewskimi, wpływanie na ich kształt i kierunki działania;
- wzmacnianie potencjału informacyjnego NATO;
- wykorzystanie działań reformujących WPZiB UE, w tym przyjęcia nowej Strategii Bezpieczeństwa UE;
- aktywna polityka informacyjna RP na forach międzynarodowych.

3. KONCEPCJA ZADAŃ OPERACYJNYCH W ZAKRESIE BEZPIECZEŃSTWA INFORMACYJNEGO RP

28. Zadania operacyjne w zakresie efektywności walki informacyjnej powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego, obywatelskiego oraz w wymiarze transsektorowym.
29. W ramach opracowania zadań operacyjnych niezbędne jest wskazanie mechanizmów przeciwdziałania wykorzystywaniu wojny informacyjnej w celach polityczno-wojskowych naruszających prawo międzynarodowe oraz przeprowadzania wrogich działań i aktów agresji stanowiących zagrożenie dla międzynarodowego bezpieczeństwa i stabilności strategicznej.
30. Do głównych zadań sektora publicznego w wymiarze krajowym należą:
    - rozpoznawanie środowiska informacyjnego (m.in. określenie podmiotów przyjaznych, neutralnych i wrogich) oraz analiza i ocena zagrożeń środowiska informacyjnego (w tym potencjalnych celów oraz możliwych do użycia kanałów informacyjnych);
    - prognoza skuteczności planowanych działań;
    - prowadzenie analizy ryzyka i prognoz dotyczących zagrożeń dla bezpieczeństwa informacyjnego;
    - opracowanie systemu monitoringu potencjalnych zagrożeń oraz efektywnego systemu przeciwdziałania zidentyfikowanym zagrożeniom, w tym wymiany danych i informacji;
    - współpraca z sektorem prywatnym w zakresie przeciwdziałania zagrożeniom;
    - planowanie użycia środków oddziaływania na środowisko informacyjne;
    - właściwe wykorzystywanie synergii powstałej w wyniku współpracy i koordynacji działań pomiędzy podmiotami różnych sektorów bezpieczeństwa narodowego i społeczeństwa obywatelskiego;
    - wdrożenie efektywnego i akceptowalnego społecznie systemu identyfikacji źródeł przekazów informacyjnych;
    - zapewnienie funkcjonowania spójnego systemu monitorowania i dystrybucji informacji w wymiarze cywilnym i wojskowym;
    - wspieranie działań mających na celu umacnianie tożsamości narodowej;
    - prowadzenie kampanii społecznych mających pozytywnie wpłynąć na obraz Polski; podejmowanie walki z propagandą ukazującą Polskę w negatywnym kontekście;
    - działania z zakresu komunikacji społecznej budujące markę RP; wykorzystanie potencjału dyplomacji publicznej;
    - prowadzenie działań zmierzających do zabezpieczenia informacyjnego strategicznych organizacji i spółek, których działanie wpływa bezpośrednio lub pośrednio na stan bezpieczeństwa narodowego Polski;

- zapobieganie, w ramach działań kontrwywiadowczych, aktywizacji przez obce państwo wybranych grup społecznych, celem realizacji interesów sprzecznych z interesem RP;
- stworzenie społecznej zdolności do rozpoznawania i neutralizacji dezinformacji; aktywizacja kapitału społecznego;
- wdrażanie mechanizmów kontrinformacji oraz edukacja i uświadamianie obywateli na poziomie narodowym m.in. poprzez zaangażowanie mediów;
- planowanie użycia i produkcji środków oddziaływania na środowisko informacyjne.

31. Główne zadania sektora publicznego na poziomie międzynarodowym:
    - aktywne uczestnictwo w projektach i przedsięwzięciach międzynarodowych na rzecz bezpieczeństwa informacyjnego, organizowanych zarówno w ramach NATO jak i UE oraz innych organizacji, których Polska jest aktywnym członkiem i które są zgodne z interesem narodowym;
    - prowadzenie aktywnej, jednolitej i spójnej polityki zagranicznej RP na forach międzynarodowych (szczególny nacisk na spójny przekaz informacyjny instytucji w kluczowych dla kraju kwestiach);
    - wspieranie procesów służących wzmocnieniu bezpieczeństwa informacyjnego Sojuszu Północnoatlantyckiego i UE;
    - gromadzenie wiedzy i doświadczeń oraz porównywanie narodowych regulacji z rozwiązaniami stosowanymi przez inne państwa, dotyczących działań z zakresu bezpieczeństwa informacyjnego;
    - wymiana doświadczeń i dobrych praktyk oraz wykorzystanie wsparcia informacyjnego partnerów/sojuszników na arenie międzynarodowej;
    - udział w międzynarodowym reagowaniu na zagrożenia bezpieczeństwa informacyjnego;
    - efektywne funkcjonowanie w sojuszniczym systemie komunikacji strategicznej, w tym wymiana informacji w zakresie zagrożeń o charakterze globalnym;
    - właściwe wykorzystywanie synergii powstałej w wyniku koordynacji działań rozproszonych (współpracy międzynarodowej);
    - odpowiednie wykorzystywanie potencjału dyplomacji publicznej poszczególnych państw;
    - objęcie mniejszości polskiej w regionie powszechnym dostępem do wszystkich polskich mediów elektronicznych (radio i tv); tworzenie silnej konkurencji dla mediów rosyjskich jako głównego przekaźnika informacji (propagandy) dla tej grupy ludności; współdziałanie z krajami regionu w zakresie nadawania programów radiowych i telewizyjnych na Białorusi;
    - dotarcie z polskimi programami informacyjnymi (radiowymi i telewizyjnymi) do mniejszości polskiej w innych krajach; objęcie tej mniejszości programami edukacyjnymi w zakresie historii i współczesnej polityki;
    - stały monitoring przekazu propagandowego ukierunkowanego na Polskę i treści dyskredytujących polską politykę zagraniczną; analiza pozwalająca identyfikować źródła przekazu oraz - na ile to możliwe - eliminowanie źródeł dezinformacji;
    - budowa i utrwalenie wizerunku Polski na arenie międzynarodowej jako podmiotu przewidywalnego, o określonych zdolnościach, m.in. do budowania koalicji w zakresie rozwiązań będących we wspólnym interesie kilku państw;

- przeciwdziałanie dezinformacji w ramach obowiązującego prawa, merytoryczna i przekonująca argumentacja polskiej narracji na forach międzynarodowych, akcentująca zaangażowanie RP we wspólne projekty.

32. Główne zadania sektora prywatnego:
    - współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom środowiska informacyjnego;
    - włączenie prywatnych nadawców komercyjnych do realizacji zadań informacyjnych stawianych mediom publicznym wobec mniejszości polskiej np. na Litwie (system zachęt i ulg podatkowych);
    - udział w mechanizmach wymiany informacji, szkoleniach, oraz stosowanie zasad dobrych praktyk;
    - aktywność i rzetelność informacyjna wobec organów odpowiedzialnych za nadzór nad funkcjonowaniem strategicznych organizacji oraz spółek państwa.
33. Główne zadania sektora obywatelskiego:
    - działania wspierające bezpieczeństwo informacyjne państwa (udział w zapewnianiu bezpieczeństwa sektora publicznego i prywatnego);
    - kreowanie spójnego przekazu służącego interesom Polski;
    - zaangażowanie obywateli oraz udział w przedsięwzięciach i ruchach obywatelskich służących wzmocnieniu bezpieczeństwa informacyjnego;
    - samoorganizacja społeczeństwa obywatelskiego poprzez samokształcenie, podnoszenie świadomości o zagrożeniach i wspieranie obywatelskiego potencjału przeciwdziałania (np. tzw. „dobre trolle”);
    - świadome konsumowanie treści informacyjnych, analiza treści (identyfikacja ataków propagandowych i dezinformacyjnych).
34. Główne zadania transsektorowe:
    - wypracowanie mechanizmów efektywnej współpracy transsektorowej;
    - bieżąca analiza środowiska bezpieczeństwa informacyjnego państwa;
    - transsektorowa koordynacja realizacji zadań podmiotów sektora publicznego i prywatnego w dziedzinie walki informacyjnej;
    - doskonalenie systemu przeciwdziałania zidentyfikowanym zagrożeniom w obszarze bezpieczeństwa informacyjnego, w tym wymiany danych i kluczowych informacji;
    - angażowanie kluczowych komunikatorów w propagowanie jednolitego przekazu;
    - współpraca sektora państwowego (służby, wojsko, administracja na wszystkich szczeblach) z mediami w celu lepszej ochrony interesów państwa w sferze informacyjnej;
    - przeciwdziałanie propagandzie oraz reagowanie kryzysowe z wykorzystaniem potencjału społecznego;
    - właściwe kreowanie postaw społecznych na rzecz bezpieczeństwa narodowego;
    - ustanawianie standardów i dobrych praktyk służących osiąganiu celów strategicznych w zakresie bezpieczeństwa informacyjnego.

4. KONCEPCJA ZADAŃ PREPARACYJNYCH (PRZYGOTOWAWCZYCH) W DZIEDZINIE BEZPIECZEŃSTWA INFORMACYJNEGO (UTRZYMANIE I ROZWÓJ SYSTEMU BEZPIECZEŃSTWA INFORMACYJNEGO RP)

35. Podstawowym zadaniem preparacyjnym określającym kierunek działania w zakresie utrzymania i rozwoju systemu bezpieczeństwa informacyjnego RP jest integracja systemu walki informacyjnej, jako elementu w systemu bezpieczeństwa narodowego, przede wszystkim poprzez utrzymywanie i doskonalenie instytucji służących realizacji zadań w zakresie bezpieczeństwa informacyjnego.
36. Aby było to możliwe, konieczne jest dokonanie stosownej reformy regulacji w polskim systemie legislacyjnym, z uwzględnieniem zagadnień takich jak:
    - stworzenie prawnych podstaw instytucjonalnej koordynacji działań w zakresie bezpieczeństwa informacyjnego;
    - opracowanie rozwiązań umożliwiających przeciwdziałanie zagrożeniom informacyjnym przez właściwe podmioty (zdolności ofensywne i defensywne);
    - opracowanie i wdrożenie norm regulujących relacje państwa, mediów publicznych i innych ośrodków informacyjnych w zakresie bezpieczeństwa informacyjnego RP.
37. Zbudowanie kompleksowego systemu umożliwiającego realizację zadań z zakresu polityki informacyjnej państwa (sektora cywilnego i militarnego).
38. Stworzenie (lub wykorzystanie istniejącego) organu pomocniczego Rady Ministrów o kompetencjach doradczych, konsultacyjnych i koordynacyjnych, odpowiedzialnego za analizę zagrożeń i opracowywanie zasad bieżącej i długofalowej polityki informacyjnej państwa.
39. Doskonalenie procedur, zasad i norm zmierzających do usprawnienia pracy organów odpowiedzialnych za ochronę obywateli w zakresie bezpieczeństwa informacyjnego.
40. Zabezpieczenie finansowe działań służących prowadzeniu polityki informacyjnej państwa.
41. Polskie rozwiązania w zakresie bezpieczeństwa informacyjnego należy kształtować w zgodzie z dokumentami UE i NATO oraz innymi inicjatywami międzynarodowymi, aby były one spójne i kompatybilne z systemami państw sojuszniczych oraz organizacji międzynarodowych, których członkiem jest Polska.

4.1. PODSYSTEM KIEROWANIA

42. Konieczne jest utworzenie i rozwijanie instytucji koordynującej działania prowadzone w ramach bezpieczeństwa informacyjnego we wszystkich sektorach bezpieczeństwa narodowego oraz budowanie zintegrowanego systemu przeciwdziałania zagrożeniom w środowisku informacyjnym.
43. Instytucja koordynująca powinna odpowiadać za realizację zadań związanych z bezpieczeństwem informacyjnym państwa, w tym:
    - wypracowanie krajowej strategii przeciwdziałania zagrożeniom informacyjnym;
    - zadania planistyczne w zakresie kierunków rozwoju polityki informacyjnej państwa;
    - koordynację wysiłków zaangażowanych sektorów w kontekście szeroko rozumianej polityki informacyjnej państwa;
    - integrację wysiłku informacyjnego sektora cywilnego i militarnego, w celu osiągnięcia efektu synergii działań;
    - doskonalenie i rozwój teorii prowadzenia polityki informacyjnej państwa umożliwiającej zapewnienie realizacji interesów narodowych;

- konsolidowanie potencjału intelektualnego w zakresie działań informacyjnych;
- zapewnianie efektywnej płaszczyzny porozumienia i budowy dobrych praktyk w zakresie współpracy poszczególnych ogniw operacyjnych.

4.2. OGNIWA OPERACYJNE

44. Niezbędne jest stworzenie i rozwijanie mechanizmów (struktur wyposażonych w odpowiednie siły, środki i zdolności) adaptujących się do środowiska w razie konieczności reagowania na pojawiające się zagrożenia informacyjne, zdolnych do rozpoznania, analizy i oceny zagrożeń informacyjnych:
    - rozbudowa narodowego systemu komunikacji strategicznej, w tym stworzenie instrumentów przeciwdziałania efektom agresji informacyjnej przeciwnika;
    - implementacja zmian organizacyjno-strukturalnych oraz technicznych w zakresie walki informacyjnej;
    - jasne określenie organów/jednostek/komórek - oraz ich kompetencji - odpowiedzialnych za utrzymanie stanu bezpieczeństwa informacyjnego, które będą rozliczane z określonych wyników (np. raporty z monitoringu);
    - stworzenie struktur wewnątrz Sił Zbrojnych RP i rozwój ich zdolności w zakresie przeciwdziałania zagrożeniom hybrydowym (np. Centrum Operacji Komunikacyjnych), w szczególności rozwijanie zdolności planowania i kierowania oraz reakcji w zakresie walki informacyjnej, zarówno o charakterze ofensywnym, jak i defensywnym;
    - powołanie zespołów funkcyjnych odpowiedzialnych za bieżące monitorowanie i odpowiednio szybkie reagowanie wobec powstających zagrożeń informacyjnych;
    - rozwijanie zdolności służb specjalnych do prowadzenia w ramach wojen hybrydowych działań o charakterze informacyjnym, zarówno o charakterze ofensywnym, jak i defensywnym;
    - budowa zdolności i narodowych struktur do przeciwdziałania zagrożeniom (operacje informacyjne i psychologiczne);
    - rozwój zdolności w zakresie ochrony danych osobowych obywateli przed naruszeniami;
    - budowa zdolności oddziaływania na grupy odbiorców w strefie wpływów potencjalnego agresora;
    - zapewnienie spójności działań służących bezpieczeństwu informacyjnemu pomiędzy ogniwami wsparcia a pozostałymi ogniwami prowadzącymi operacje komunikacyjne.
45. Istnieje potrzeba wypracowania stosownych mechanizmów i procedur działania w zakresie bezpieczeństwa informacyjnego:
    - opracowanie procedur planowania, organizowania, koordynacji i nadzoru w sferze bezpieczeństwa informacyjnego;
    - opracowanie procedur działania oraz kompetencji poszczególnych organów na wypadek zagrożenia informacyjnego (w zakresie działań pasywnych i aktywnych);
    - organizacja systemu szkolenia kadr w zakresie bezpieczeństwa informacyjnego.
46. Potrzebna jest optymalizacja działań informacyjnych w wymiarze międzynarodowym:
    - rozwój zdolności polskiej dyplomacji w zakresie prowadzenia walki informacyjnej i promowania stanowiska Polski na formatach sojuszniczych;

- dostosowanie do standardów bezpieczeństwa informacyjnego wykorzystywanych przez organizacje międzynarodowe takie jak NATO i UE;
- opracowanie rozwiązań doktrynalnych spójnych z rozwiązaniami sojuszniczymi.

47. Potrzebne jest wypracowanie rozwiązań pozwalających na wykorzystanie potencjału mediów, sektora prywatnego i społeczeństwa obywatelskiego:
    - wzmocnienie zdolności Ministerstwa Obrony Narodowej, Ministerstwa Kultury i Dziedzictwa Narodowego, Ministerstwa Edukacji Narodowej i Ministerstwa Nauki i Szkolnictwa Wyższego w zakresie realizacji zadań służących kształtowaniu postaw patriotycznych, proobronnych i propaństwowych oraz edukacji w zakresie ochrony praw człowieka i obywatela;
    - utrzymanie i doskonalenie systemu narzędzi kształtowania świadomości społecznej, zgodnie z celami polityki informacyjnej państwa oraz interesem narodowym, w tym uruchomienie właściwych mechanizmów pozwalających dbać o poziom świadomości społecznej (spoty, media społecznościowe i inne formy przekazu);
    - opracowanie procedur współpracy z mediami – bieżącej i w stanach zagrożenia – oraz opracowanie zasad/wytycznych doboru mediów w celu realizacji operacji komunikacyjnych wykorzystujących potencjał mediów masowych, a także współpracy z nimi w zakresie realizacji zadań z obszaru walki informacyjnej;
    - zwiększenie efektywności przekazu informacyjnego i zaspokajania potrzeb informacyjnych mediów przez służby prasowe/informacyjne poszczególnych ogniw rządowych, w szczególności poprzez zacieśnienie współpracy administracji i służb z mediami;
    - stworzenie i utrzymanie kanałów szybkiego dostępu do kluczowych mediów masowych w kraju i za granicą.

4.3. PUBLICZNE I PRYWATNE OGNIWA WSPARCIA

48. Istnieje potrzeba zapewnienia spójności działań służących bezpieczeństwu informacyjnemu pomiędzy ogniwami wsparcia a pozostałymi elementami prowadzącymi operacje komunikacyjne, dlatego konieczne jest zapewnienie mechanizmów współpracy międzyresortowej i partnerstwa publiczno-prywatnego w tym zakresie.
49. Potrzebne jest wypracowanie zasad, kierunków i form organizacyjnych edukacji dla bezpieczeństwa, kształtowania postaw patriotycznych, proobronnych, świadomości bezpieczeństwa narodowego, wsparcia dla inicjatyw społecznych, w tym budowy więzi Sił Zbrojnych RP i pozostałych struktur bezpieczeństwa ze społeczeństwem.
50. Istotnym elementem dbałości o bezpieczeństwo informacyjne RP jest wykorzystanie zdolności społeczeństwa do prowadzenia rozproszonych działań w zakresie walki informacyjnej w cyberprzestrzeni. Należy zadbać o rozwój społeczeństwa obywatelskiego i włączenie go do systemu bezpieczeństwa narodowego w zakresie walki informacyjnej poprzez:
    - zapobieganie zjawisku wykluczenia informacyjnego;
    - zaangażowanie społeczeństwa w kraju oraz Polonii w proces weryfikowania odbieranych przekazów informacyjnych;
    - opracowanie koncepcji budżetowej w zakresie wsparcia organizacji służących zapewnieniu tożsamości narodowej i dziedzictwa kulturowego, promujących postawy patriotyczne i proobronne w duchu polskiej racji stanu;

- opracowanie planów i programów działania zmierzających do utrzymania odpowiedniej zdolności funkcjonowania społeczeństwa w czasie zagrożenia;
- utworzenie katalogu inicjatyw kulturalnych wchodzących w skład przedsięwzięć wspierających politykę informacyjną państwa w duchu polskiego interesu narodowego.

51. Niezbędne jest promowanie rozwoju narodowej myśli technicznej w zakresie doskonalenia zdolności ochrony, obrony i rażenia w kontekście środowiska informacyjnego:
    - stymulowanie przez państwo rozwoju badań naukowych nad bezpieczeństwem;
    - utworzenie pozarządowej instytucji badawczej realizującej zadania własne, zlecenia organów i instytucji państwa oraz podmiotów publicznych w zakresie bezpieczeństwa narodowego (ukierunkowanych na kwestie bezpieczeństwa informacyjnego).
52. Potrzebne jest stworzenie silnego kanału komunikacyjnego do prowadzenia walki informacyjnej (m.in. na drodze przekształceń programowych TVP Polonia, wykorzystania Internetu itp.).

ZAKOŃCZENIE

53. Doktryna bezpieczeństwa informacyjnego RP – jako transsektorowy dokument wykonawczy do Strategii Bezpieczeństwa Narodowego RP – stanowi podstawę koncepcyjną do przygotowania i realizacji skoordynowanych w skali państwa działań dla bezpieczeństwa informacyjnego RP, sektora publicznego i sektora prywatnego.
54. Rekomendacje niniejszej Doktryny przeznaczone są do odpowiedniego wykorzystania przez wszystkie podmioty publiczne i prywatne odpowiedzialne za planowanie, organizowanie i realizowanie zadań w dziedzinie bezpieczeństwa informacyjnego.
55. Treść Doktryny powinna być rozwinięta przede wszystkim w kolejnej Polityczno-Strategicznej Dyrektywie Obronnej oraz w kolejnej edycji Strategii (Programu) Rozwoju Systemu Bezpieczeństwa Narodowego, a także w planach zarządzania kryzysowego oraz operacyjnych planach funkcjonowania struktur państwa w czasie zagrożenia i wojny, jak również w programach rozwoju sił zbrojnych i programach pozamilitarnych przygotowań obronnych.

GENERALNE ZAŁOŻENIA NARODOWEGO PROGRAMU SYSTEMÓW BEZZAŁOGOWYCH

W 2014 r., na polecenie Prezydenta RP Bronisława Komorowskiego, w BBN podjęto prace nad opracowaniem Narodowego Programu Systemów Bezzałogowych.

Celem prac było wsparcie rodzimej produkcji bezzałogowców, uzyskanie politycznej i społecznej akceptacji dla rozwoju tej gałęzi przemysłu oraz opracowanie strategii jej rozwoju w Polsce.

W pracach nad programem wzięli udział przedstawiciele politechnik i instytutów badawczych reprezentujących środowiska naukowe; resortów, poszczególnych służb i państwowych przedsiębiorstw reprezentujących obecnych i potencjalnych użytkowników; a także producenci systemów bezzałogowych.

Założenia zostały przekazane do Ministerstwa Obrony Narodowej w lipcu 2015 r.

22 lipca 2015 r.

GENERALNE ZAŁOŻENIA NARODOWEGO PROGRAMU SYSTEMÓW BEZZAŁOGOWYCH

Aby zapewnić właściwy rozwój nowej polskiej specjalności ustanawia się Narodowy Program Systemów Bezzałogowych. Program ten zdefiniuje cele i zadania oraz ramy organizacyjne, finansowe, a także prawne.

I. Cele ustanowienia Narodowego Programu Systemów Bezzałogowych (NPSB)

1. Jako **cele główne** (strategiczne) *Narodowego Programu Systemów Bezzałogowych* należy przyjąć:
   - Opracowanie systemu wsparcia dla rozwoju rodzimej produkcji bezzałogowców w obszarach kluczowych dla naszego bezpieczeństwa;
   - Stworzenie polskiej specjalności gospodarczej w zakresie budowy i komercjalizacji systemów bezzałogowych.
2. Do **celów pośrednich**, należy zaliczyć:
   - Opracowanie długofalowej strategii wspierania rozwoju systemów bezzałogowych i robotycznych kluczowych dla bezpieczeństwa narodowego oraz rozwoju społeczno-gospodarczego Polski, w tym:
     - Zdefiniowanie ram organizacyjnych, finansowych i prawnych dla rozwoju polskich systemów bezzałogowych i robotycznych,
     - Zbudowanie świadomości konieczności rozwoju rodzimych systemów bezzałogowych i robotycznych,
     - Pobudzenie popytu na rodzime rozwiązania w zakresie robotyki, w tym systemy bezzałogowe w sektorze bezpieczeństwa narodowego,
     - Przygotowanie i wdrożenie długofalowej strategii w kontekście relacji człowiek - maszyna - społeczeństwo.
   - Stworzenie platformy dialogu i szerokiej wymiany informacji pomiędzy środowiskami odpowiedzialnymi za bezpieczeństwo, a naukowo-przemysłowymi, przy wsparciu m.in.: BBN, NCBiR, czyli:
     - Opracowanie księgi popytu i podaży dla systemów bezzałogowych na potrzeby zarządzania i ochrony infrastrukturą o strategicznym znaczeniu dla bezpieczeństwa państwa (na najbliższe 20 lat),
     - Skonsolidowanie środowisk i ułatwienie ich przedstawicielom racjonalnej współpracy,

- Pobudzenie popytu na rodzime rozwiązania w zakresie robotyki, w tym systemy bezzałogowe w sektorze bezpieczeństwa narodowego,
- Konsultacje z instytucjami rządowymi oraz przedsiębiorstwami państwowymi, zmierzające do oszacowania przez powyższe, korzyści z implementacji systemów bezzałogowych - robotów.

- Pobudzenie dialogu i szerokiej wymiany informacji pomiędzy środowiskami odpowiedzialnymi za rozwój technologiczny, tj.: nauki, przemysłu, użytkowników, NCBiR, ULC, Ministerstwa Gospodarki, Ministerstwa Nauki i Szkolnictwa Wyższego, Ministerstwa Administracji i Cyfryzacji, itp., tj.:
  - konsolidacja środowisk i zapewnienie ich przedstawicielom racjonalnej współpracy poprzez wsparcie dla działań Polskiej Platformy Technologicznej Systemów Bezzałogowych i Polskiej Platformy Systemów Bezpieczeństwa,
  - określenie obecnych możliwości i zdolności badawczych oraz rozwojowych środowisk naukowo-przemysłowych,
- Ustanowienie programów:
  - sektorowego finansowania przez NCBiR - integrującego przedsiębiorstwa, jednostki naukowe i użytkowników końcowych wokół rozwoju pełnej gamy cywilnych systemów bezzałogowych powietrznych, lądowych i morskich,
  - komplementarnego do ww., finansowanego przez NCBiR w obszarze bezpieczeństwa i obronności państwa integrującego przedsiębiorstwa, jednostki naukowe i użytkowników końcowych wokół rozwoju systemów bezzałogowych w zastosowaniach militarnych,
- Zintensyfikowanie współpracy na poziomie międzynarodowym z partnerami przemysłowymi i badawczymi w zakresie rozwoju systemów bezzałogowych i robotycznych,
- Przygotowanie na uczelniach wyższych programów kształcenia wysokiej klasy specjalistów w zakresie systemów bezzałogowych i ich komponentów (telekomunikacja, informatyka, kryptologia, nawigacja, mechatronika, zaawansowane materiały).
- Uzyskanie społecznej akceptacji rozwoju robotyki, jako dziedziny nauki, rozwoju narodowej gospodarki i zjawiska społecznego w Polsce.
- Wspieranie nowego, innowacyjnego sektora nauki i gospodarki poprzez odpowiednie zmiany w obowiązującym prawie.

II. Kierowanie NPSB

W celu realizacji NPSB przy Premierze powstałaby **Rada Programowa** kierowana przez Przewodniczącego Rady - Prezesa Rady Ministrów (lub szefa Kancelarii Prezesa Rady Ministrów) z udziałem wiceministrów resortów najbardziej zainteresowanych przyszłym użytkowaniem systemów bezzałogowych (MON, MG, MSW, MIiR, MAiC, MNiSW, MSZ,) oraz Szefa BBN.

Organem wykonawczym Rady Programowej byłby **Komitet Sterujący** (KS) - w sumie 21 osób - powinien być organem wykonawczym Rady.

- Przewodniczący (**1**):
- Zastępcy przewodniczącego (**7**):
  - Politechnika Warszawska (1),

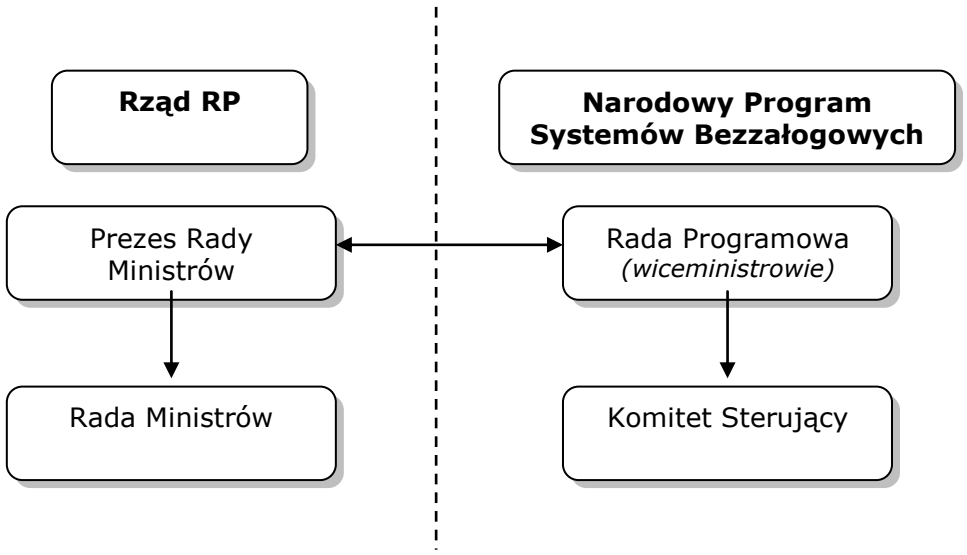
- Polska Grupa Zbrojeniowa (1),
- Instytut Techniczny Wojsk Lotniczych (1),
- Centrum Techniki Morskiej (1),
- Przemysłowy Instytut Automatyki i Pomiarów (1),
- WB Electronics (1),
- przedstawiciel MON (1),

- Członkowie KS (**13**):
  - przedstawiciel BBN (1),
  - przedstawiciele MG, MSW, MIiR, MAiC, MNiSW, MSZ (6),
  - przedstawiciele Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego (2);
  - przedstawiciele nauki i przemysłu reprezentujący obszary bezzałogowych systemów lądowych, latających i pływających (4).

Komitet Sterujący byłby jednocześnie organem doradczym Rady Programowej, która miałaby głos decydujący w ustanawianiu aktywności. Komitet Sterujący mógłby wskazać i nadzorować te podmioty/zespoły, które po rekomendacji przez KS zostałyby wskazane do realizacji przedsięwzięć wskazanych w jego zadaniach, po zatwierdzeniu przez Radę.

NCBiR byłby podmiotem realizującym programy/projekty zgodnie z mechanizmami zapisanymi w ustawie o NCBiR.

Rada Programowa, nie rzadziej niż raz w roku (poprzez Przewodniczącego Rady) sprawozdawałaby Prezydentowi, po zatwierdzeniu sprawozdania przez Premiera.



Schemat ilustrujący umiejscowienie NPSB modelu kierowania nim w strukturze Państwa

Zadania Komitetu Sterującego

Najważniejszymi zadaniami, jakie staną przed Komitetem będą:

1. Opracowanie koncepcji i założeń *Narodowego Programu Systemów Bezzałogowych*. Komitet Sterujący powinien wypracować cele programu, przekonać do ich realizacji

władze państwowe a następnie zorganizować odpowiednie zespoły tematyczne i nadzorować realizację przyjętego harmonogramu.

2. Analiza potrzeb poszczególnych resortów i gałęzi gospodarki w zakresie wykorzystania platform bezzałogowych.
3. Przegląd technologii jaki są niezbędne dla rozwoju systemów bezzałogowych w Polsce. Wskazanie priorytetowych technologii, na podstawie których realizowane będą przyszłe projekty bezzałogowe. Określony poziom technologiczny będzie osiągany w wyniku zintensyfikowanego procesu finansowania prac badawczo-rozwojowych, a także w wyniku pozyskiwania tych technologii w ramach współpracy międzynarodowej.
4. Skatalogowanie posiadanych już produktów, technologii, usług, a wreszcie zdolności związanych z systemami bezzałogowymi. Ocena stopnia zawansowania prac krajowych nad niezbędnymi technologiami zarówno dostępnymi w przemyśle jak i opracowywanymi przez ośrodki naukowe. Ocena dostępności niezbędnych technologii ze źródeł zagranicznych.
5. Zdefiniowanie barier prawnych, uniemożliwiających eksploatację systemów bezzałogowych różnorakiego przeznaczenia oraz zainicjowanie prac legislacyjnych, zmierzających do usankcjonowania aspektów prawnych.
6. Dialog oraz szeroka wymiana informacji (*w przypadku Sił Zbrojnych RP objęte określona klauzulą niejawności*) z poszczególnymi użytkownikami platform bezzałogowych.
7. Zarządzanie środkami, w tym finansowymi, pozyskiwanymi na realizację i rozwój projektów, będących wynikiem konsultacji z użytkownikami i zdefiniowanymi oczekiwaniami.
8. Wskazywanie i monitorowanie procesu kształcenia oraz rozwoju kadr na przykład inżynierskich czy menedżerskich będących w stanie realizować i kierować przygotowywanymi projektami.
9. Powoływanie w razie potrzeby paneli eksperckich, na zasadzie konsultacji i doradztwa (inwestycyjnego, informatycznego, zawodowego, finansowego, prawnego, itd.). Zakres odpowiedzialności oraz skład paneli ekspertów będzie w sposób naturalny odzwierciedlać zakres działania perspektywicznego. Różne sposoby rekrutacji uczestników panelu uwzględnią zaś dwie zasady - różnorodności (wiedzy/poglądów) oraz równowagi (różnych postaw/poglądów).

REKOMENDACJE BBN WS. ROLI ORGANIZACJI POZARZĄDOWYCH WE WZMACNIANIU STRATEGICZNEJ ODPORNOŚCI KRAJU

Jednym z ważnych elementów przygotowanej przez Biuro Bezpieczeństwa Narodowego koncepcji strategicznej odpornosci kraju na agresję było wykorzystanie potencjału oraz aktywności społecznych organizacji proobronnych.

W ramach prac nad koncepcją w BBN odbyło się kilkanaście spotkań, m.in. z udziałem przedstawicieli organizacji proobronnych. Obok stosownych rekomendacji Biuro przygotowalo również tzw. Katalog Potrzeb i Możliwości. Zostały w nim zawarte propozycje zadań dla organizacji – zarówno na czas pokoju i kryzysu, a także w pewnym zakresie na czas wojny.

4 lutego 2015 r. rekomendacje BBN zostały przekazane do Ministerstwa Obrony Narodowej, jako instytucji wiodącej we współpracy z organizacjami proobronnymi.

BIURO BEZPIECZEŃSTWA NARODOWEGO

4 lutego 2015 r.

REKOMENDACJE BBN WS. ROLI ORGANIZACJI POZARZĄDOWYCH WE WZMACNIANIU STRATEGICZNEJ ODPORNOŚCI KRAJU

Wstęp

Jednym z głównych elementów systemu obrony państwa – obok działań regularnych sił zbrojnych – jest strategiczna odporność kraju na agresję. Składają się na nią działania militarne i niemilitarne zwiększające niedostępność terytorium, powszechność przygotowań obronnych pozamilitarnych struktur państwa, a także skuteczność wsparcia sił zbrojnych, w tym możliwość zorganizowanego oporu na terenach zajętych przez agresora. Odpowiedni poziom strategicznej odporności kraju może być istotnym czynnikiem odstraszania.

Ważną rolę w tym systemie mogą i powinny pełnić organizacje pozarządowe (NGO) o charakterze proobronnym, które w momencie kryzysu lub wojny stanowiłyby istotne uzupełnienie i wsparcie zarówno dla pozamilitarnych, jak i militarnych struktur państwa. Realizując wytyczne Prezydenta RP, Bronisława Komorowskiego, Biuro Bezpieczeństwa Narodowego podjęło prace nad zdefiniowaniem roli i miejsca tych organizacji we wzmacnianiu strategicznej odporności kraju (na agresję) w ramach zintegrowanego systemu bezpieczeństwa narodowego.

W BBN przeprowadzono szereg konsultacji społecznych w formule Strategicznego Forum Bezpieczeństwa (SFB), m.in.: 30 kwietnia, 8 lipca, 30 września 2014 r. oraz 12 stycznia 2015 r., poświęconych wzmacnianiu strategicznej odporności kraju poprzez szersze wykorzystanie potencjału organizacji pozarządowych. Spotkania te stworzyły możliwość skonfrontowania przyjętych założeń, a także wzajemnych oczekiwań organizacji pozarządowych oraz organów i instytucji państwowych.

W toku dyskusji podkreślano znaczenie budowania proobronnej świadomości społecznej: upowszechniania stosownej wiedzy (edukacja dla obronności), kształtowania i wykorzystania postaw proobronnych i patriotycznych - dla strategicznej odporności kraju. Zwracano uwagę na implikacje zachowania się społeczeństwa w sytuacji kryzysu lub zagrożenia wojennego oraz znaczenie strategicznej komunikacji ze społeczeństwem – ważnego elementu strategicznej odporności kraju (ludności, środków masowego przekazu, itp.) – na agresję informacyjno-propagandową. Podnoszono problem inspirowania zainteresowania wojskiem i sprawami obronności (rodzina-szkoła-wojsko). Projekt zaangażowania organizacji pozarządowych, w tym organizacji o charakterze proobronnym we wzmacnianie bezpieczeństwa państwa, wpisuje się w postulaty przyjętej przez Radę Ministrów w 2013 r. "*Strategii rozwoju systemu*

bezpieczeństwa narodowego RP 2022", a przede wszystkim, stanowi implementację Strategii Bezpieczeństwa Narodowego, zatwierdzonej przez Prezydenta RP 5 listopada 2014 r.[1]

W trakcie kolejnych spotkań SFB uzgodniono potrzebę opracowania Katalogu Potrzeb i Możliwości, definiującego z jednej strony potrzeby państwa w zakresie obszarów potencjalnego wykorzystania i zadań dla konkretnych organizacji pozarządowych (potrzeby operacyjne, szkoleniowe, itd.), z drugiej – zdolności i możliwości, ale także oczekiwania i warunki zaangażowania tych organizacji we wzmacnianie strategicznej odporności kraju (czyli jakie działania organizacje pozarządowe mogą i pragną dobrowolnie podejmować na rzecz państwa).

Wdrażając wnioski z przeprowadzonych konsultacji, Szef BBN zwrócił się 17 października 2014 r. do poszczególnych ministerstw, instytucji oraz służb, realizujących ustawowe zadania z dziedziny bezpieczeństwa i obronności, z prośbą o rekomendacje dotyczące Katalogu w zakresie potrzeb identyfikowanych przez te instytucje. Uzyskane odpowiedzi i reakcje zwrotne pozwalają stwierdzić, że idea wykorzystania potencjału organizacji pozarządowych we wzmacnianie strategicznej odporności kraju została uznana za uzasadnioną – spotkała się ze zrozumieniem i pozytywnym przyjęciem, chociaż nie wszystkie instytucje przykładają do niej równie dużą wagę.

Najszerzej do prośby BBN odniosło się Ministerstwo Obrony Narodowej, które przedstawiło merytoryczne propozycje, mogące stanowić punkt wyjścia do dalszych prac. MON bazowało na wieloletnich doświadczeniach ze współpracy z organizacjami pozarządowymi, które zaowocowały stworzeniem odpowiednich narzędzi organizacyjno-prawnych. Konstruktywny wkład do stanowiska MON wniosły dodatkowo zarówno SG WP, dowództwa RSZ, jak i departamenty ministerstwa (zwłaszcza Departament Strategii i Planowania Obronnego oraz Departament Wychowania i Promocji Obronności). MON skorzystało także z wiedzy eksperckiej szkół i akademii wojskowych.

Na podkreślenie zasługuje również fakt, że inicjatywa podjęta przez BBN została wsparta praktycznymi działaniami przez Ministra Obrony Narodowej, który decyzją Nr 460/MON z 20 listopada 2014 r. powołał Pełnomocnika Ministra Obrony Narodowej ds. Społecznych Inicjatyw Proobronnych, powierzając mu m.in. zadania nawiązania i koordynacji współpracy z organizacjami pozarządowymi o charakterze proobronnym oraz przygotowania w resorcie obrony narodowej propozycji nowych, systemowych rozwiązań. Minister ON upoważnił również Pełnomocnika do powołania nieetatowego Zespołu ds. Społecznych Inicjatyw Proobronnych zalecając, aby ww. Zespół nawiązał współpracę z Biurem Bezpieczeństwa Narodowego w celu wykorzystania rezultatów dotychczasowych prac.

Działania te wychodzą naprzeciw oczekiwaniom przedstawicieli organizacji pozarządowych, którzy w trakcie SFB wskazywali na potrzebę utworzenia organu koordynująco-integrującego ich współpracę z organami państwa.

Uwagi ogólne:

1. Uwarunkowania prawne. Zarówno konsultacje przeprowadzone w BBN w formule SFB, jak i rekomendacje instytucji państwowych wskazują, że istniejące regulacje prawne pozwalają znacznie rozszerzyć wykorzystanie organizacji pozarządowych bez daleko idących zmian ustawowych. Chodzi tu zwłaszcza o Ustawę z dnia 21 listopada 1967 r. *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (tekst jednolity Dz. U. 2012 r., poz. 461 z późn. zm.) oraz Ustawę z dnia 24 kwietnia 2003 r. *o działalności pożytku publicznego i o wolontariacie* (Dz U. 2003 nr 96 poz. 873). Wystarczające (na obecnym etapie) regulacje zawierają również ustawy: z dnia 18 kwietnia 2002 r. *o stanie klęski żywiołowej*, z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, z dnia 24 sierpnia 1991 r. o ochronie

[1] SBN zawiera 12 odniesień, które w sposób bezpośredni lub pośredni dotyczą roli i miejsca organizacji pozarządowych oraz podmiotów prywatnych w umacnianiu strategicznej odporności kraju na różnorodne zagrożenia.

przeciwpożarowej, z dnia 21 czerwca 2002 r. *o stanie wyjątkowym* oraz z dnia 27 kwietnia 2001 r. *Prawo ochrony środowiska* (Dz.U. 2001 nr 62 poz. 627).

MON rekomenduje rozszerzenie i uzupełnienie aktów wykonawczych, np. uszczegółowienie rozporządzenia Rady Ministrów z dnia 13 stycznia 2014 roku *w sprawie ogólnych zasad wykonywania zadań w ramach powszechnego obowiązku obrony* (Dz. U. Nr 16, poz. 152).

W dalszej perspektywie – w miarę doskonalenia współdziałania z organizacjami pozarządowymi – zmiany ustawowe, poprzedzone stosownym przeglądem obowiązujących aktów prawnych, wydają się być konieczne. Dotyczyć to może np. kwestii rozsądnego, uzasadnionego realnymi potrzebami, rozszerzenia i ułatwienia kwalifikowanego dostępu do broni (co postulują niektóre organizacje pozarządowe), jak również szczegółowych kompetencji w poszczególnych obszarach wsparcia państwa przez NGO.

2. Uwarunkowania finansowe. Zwiększenie zaangażowania organizacji pozarządowych we wzmacnianie Strategicznej Odporności Kraju wymaga zwiększenia środków finansowych przeznaczanych na ten cel. Skalę potrzeb ilustruje przykład MON: Minister Obrony Narodowej na realizację zadań publicznych w 2014 r. zaplanował kwotę 8 mln 920 tys. zł., podczas gdy organizacje pozarządowe złożyły 703 oferty na kwotę ponad 27 mln złotych. W 2013 r. podmioty zainteresowane pozyskaniem zbędnego w Siłach Zbrojnych RP mienia ruchomego Skarbu Państwa złożyły 906 wniosków z czego pozytywnie rozpatrzono 407. Łączna wartość przekazanego mienia wojskowego wyniosła 16 643 891,29 zł. Do tego dochodzą koszty eksploatacyjne, związane z użyczeniem obiektów i sprzętu (np. koszty transportu).

   Należy jednak zauważyć, że dotychczasowe plany współpracy MON z organizacjami pozarządowymi koncentrowały się na przedsięwzięciach promujących obronność, a nie budujących konkretne zdolności wspierające siły zbrojne lub wzmacniające strategiczną odporność kraju na ewentualną agresję. Zmiana struktury rocznych planów współpracy, a tym samym propozycji dla organizacji pozarządowych w ramach Otwartych Konkursów Ofert na zlecanie zadań publicznych w zakresie obronności państwa – to najprostszy sposób zmiany charakteru współpracy wojsko/organizacje w kierunku wzmacniania Strategicznej Odporności Kraju.

3. Doświadczenia historyczne. Już w czasach II Rzeczypospolitej – pod wpływem doświadczeń I Wojny Światowej – zdecydowano o wykorzystaniu organizacji pozarządowych: paramilitarnych, proobronnych i kombatanckich – do odpowiedniego przygotowania obronnego całego społeczeństwa oraz stworzenia systemu rezerw osobowych na potrzeby mobilizacyjne. Organizacje te prowadziły działalność zgodnie z wytycznymi wojska, a nadzór i koordynację przygotowania obronnego społeczeństwa i edukacji obronnej sprawował Państwowy Urząd Wychowania Fizycznego i Przysposobienia Wojskowego (PUWFiPW) utworzony w 1927 r. przez władze wojskowe. Z kolei, związki rezerwistów skupiała Federacja Polskich Związków Obrońców Ojczyzny (FPZOO) utworzona w 1928 r. Warto przypomnieć, że organizacje jej podległe miały często własne, niezależne od wojska pomysły tworzenia samodzielnych formacji na czas wojny. W latach 30-tych FPZOO przedstawiła np. koncepcję samodzielnego wystawienia "armii rezerwowej" - z własną kadrą dowódczą i zadaniami, "dopuszczając" jej podporządkowanie regularnemu wojsku[2].

4. Uwarunkowania formalno-organizacyjne (na podstawie uwag Departamentu Strategii i Planowania Obronnego MON).

   - Różnorodność organizacji pozarządowych daje szanse wykorzystania ich potencjału w ramach wzmacniania bezpieczeństwa państwa zarówno w sferze działań niemilitarnych, w tym pośrednich (oddziaływanie na społeczeństwo) i bezpośrednich (realizowanych na rzecz sił zbrojnych) oraz militarnych (operacyjnych).

[2] L. Wyszczelski, Armia Rezerwowa II Rzeczypospolitej, Bellona, Warszawa, 2014 r.

- W sferze działań niemilitarnych, w tym przede wszystkim pośrednich, potencjał, jakim dysponują organizacje pozarządowe jest wykorzystywany od wielu lat. Działania resortu obrony narodowej w tym zakresie reguluje decyzja nr 187/MON Ministra Obrony Narodowej z dnia 9 czerwca 2009 r. (Dz. Urz. MON z 2009 r. Nr 12, poz. 131 z późn. zm.).
- Obowiązujące przepisy prawa, w szczególności zapisy rozporządzenia Rady Ministrów z dnia 13 stycznia 2004 r. w sprawie ogólnych zasad wykonywania zadań w ramach powszechnego obowiązku obrony (Dz.U. z 2004 r. nr 16, poz. 152) pozwalają na wykorzystanie potencjału organizacji społecznych do realizacji zadań obronnych. Możliwość taką posiada w swych kompetencjach wojewoda, który w planie operacyjnego funkcjonowania może wskazać konkretną organizację do realizacji zadania obronnego, jako podmiot współdziałający. Realizacja takiego przedsięwzięcia wymaga podpisania stosownego porozumienia.
- Do chwili obecnej potencjał pozarządowych organizacji proobronnych w sferze bezpośrednich działań niemilitarnych nie był wykorzystywany, a w sferze działań militarnych (operacyjnych) nie rozważano nawet opcji jego wykorzystania.

W odniesieniu do dotychczasowych kierunków prac należy zaznaczyć, że:

1) Operacyjne (bojowe) wykorzystanie potencjału pozarządowych organizacji proobronnych łączy się z potrzebą włączenia ich w struktury wojskowe (jako samodzielne formacje lub elementy większej całości).
2) Narodowe Siły Rezerwowe (NSR), w skład których mogłyby wchodzić organizacje proobronne, stanowią część Sił Zbrojnych RP, które funkcjonują w ramach jednolitego systemu dowodzenia i kierowania, zaopatrywania, uzupełnień, a także innych podsystemów wykonawczych, posiadają określoną liczebność i strukturę oraz podlegają procesowi szkolenia zgodnie z obowiązującymi dokumentami doktrynalnymi.
3) Ewentualne włączenie dodatkowych elementów w strukturę Narodowych Sił Rezerwowych wiązałoby się z koniecznością dostosowania ich do obowiązujących w Siłach Zbrojnych wymogów w celu osiągnięcia odpowiedniego poziomu interoperacyjności, w tym również ujednolicenia i skonsolidowania procesu kierowania i szkolenia.
4) Wykorzystanie potencjału pozarządowych organizacji proobronnych w sferze działań militarnych (operacyjnych, bojowych) wymaga uwzględnienia takich czynników, jak:
   - określenie formuły współdziałania (włączenie w struktury militarne czy tylko ich wspieranie);
   - zapewnienie kompatybilności struktur i systemu kierowania;
   - ujednolicenie wyposażenia i logistycznego zaopatrywania;
   - skonsolidowanie procesu szkolenia;
   - zapewnienie finansowania;
   - wskazanie organu administracji sprawującego nadzór.
5) Z punktu widzenia Sił Zbrojnych RP, najbardziej pożądana byłaby formuła współpracy z jednym partnerem społecznym (np. zrzeszeniem pozarządowych organizacji proobronnych), której celem będzie wspieranie działań elementów militarnych systemu obronnego.
6) W ramach nowego cyklu planowania obronnego przewiduje się wykorzystanie kompetencji wojewodów w zakresie nakładania zadań obronnych na organizacje pozarządowe na szczeblu lokalnym (województwa) przy założeniu, że ich realizacja

będzie zgodna ze statutem organizacji, odbywać się będzie na obszarze jej działania i w oparciu o stosowne porozumienia, zarówno w przypadku zaistnienia sytuacji kryzysowych wynikających z zagrożeń niemilitarnych (szczególnie o znamionach klęsk żywiołowych), jak również w sytuacji zewnętrznego zagrożenia i w czasie wojny.

Rekomendacje BBN:

1. W pracach Zespołu MON ds. Społecznych Inicjatyw Proobronnych proponuje się rozważyć i w miarę możliwości uwzględnić, postulaty przedstawicieli organizacji pozarządowych zgłaszane w BBN, w ramach Strategicznego Forum Bezpieczeństwa, dotyczące m.in:
   - potrzeby zapewnienia większej otwartości państwa na postrzeganie roli NGO w sprawach bezpieczeństwa (partnerstwo w miejsce systemu nakazowo-rozdzielczego);
   - udostępniania organizacjom szerszej wiedzy nt. potrzeb państwa;
   - stworzenia stałej platformy współdziałania z NGO (konwent, federacja, inne?);
   - kontynuowania prac nad doskonaleniem Katalogu Potrzeb i Możliwości;
   - stworzenia zintegrowanego systemu ratownictwa, z przewidzianym, dobrowolnym wsparciem NGO;
   - wypracowania instrumentów ułatwiających samoorganizację społeczeństw lokalnych;
   - stworzenia grup kontaktowych na wzór CIMIC na poziomie województw (koordynacja zobowiązań – rola wojewody);
   - podjęcia kroków zmierzających do rozsądnej liberalizacji dostępu do broni, wprowadzenia nowych kategorii dostępu itd. (potrzebne byłyby nowe regulacje ustawowe - organizacje dysponują stosownymi projektami);
   - umożliwienia szerszego dostępu do obiektów wojskowych (poligony, strzelnice), możliwości korzystania z wyżywienia wg stawek wojska oraz przechowywania broni i amunicji dla organizacji proobronnych w jednostkach wojskowych.
2. Przykłady szczegółowych problemów sygnalizowanych przez NGO:
   - Trudności w weekendowym dostępie do obiektów szkoleniowych (niestety, wojsko ma wówczas „wolne”);
   - Rozliczanie nieobecności w pracy osób biorących udział w działaniach antykryzysowych (dotyczy to zwłaszcza krótkofalowców, zabezpieczających łączność, informowanie i powiadamianie – w ramach reagowania kryzysowego);
   - Szersze uwzględnianie (zapraszanie) NGO do udziału w ćwiczeniach i manewrach;
   - Częstsze korzystanie z formuły powierzania, a nie zlecania zadań.
3. Należy rozszerzyć zakres podmiotowy i przedmiotowy kwerendy przeprowadzonej przez BBN na potrzeby Katalogu Potrzeb i Możliwości, odnośnie do potencjalnych potrzeb państwa oraz możliwej roli proobronnych organizacji pozarządowych we wzmacnianiu Strategicznej Odporności Kraju (uwzględnić wszystkie organy i instytucje mające przyporządkowane stosowne zadania i kompetencje, a zwłaszcza terenowe organy władzy oraz samorządu terytorialnego - chodzi np. o ustawową rolę wojewody w czasie kryzysu i wojny).
4. Katalog powinien być dokumentem "żywym" i podlegać stałej aktualizacji.

5. W dalszych pracach nad Katalogiem Potrzeb i Możliwości należy rozważyć podejście analogiczne, jak w przypadku tworzenia zdolności operacyjnych Sił Zbrojnych RP (ujednolicone wytyczne, standaryzacja, jednoznaczność definicji, itp).
6. Należy dokonać przeglądu aktów prawnych w celu zidentyfikowania obszarów niezbędnych zmian (chodzi zwłaszcza o sztuczne ograniczenia oraz wyeliminowanie ewentualnych sprzeczności odnośnie do postrzegania roli NGO).
7. Należy przeanalizować zakres i mechanizm dozwolonego prawem reklamowania członków organizacji pozarządowych (wyłączenia – w uzasadnionych przypadkach – z mobilizacji w ramach powszechnego obowiązku obrony). Reklamowanie powinno jednak nadal pozostać wyjątkiem, a nie regułą.
8. Należy zidentyfikować przypadki, w których współpraca z organizacjami – ze względu na szczególne znaczenie dla obronności – powinna mieć charakter niejawny – i rozpocząć prace nad odpowiednimi regulacjami prawnymi.
9. Uwarunkowania finansowe. Zwiększenie zaangażowania organizacji pozarządowych we wzmacnianie Strategicznej Odporności Kraju wymaga zwiększenia środków finansowych.
10. Należy skorygować zakres tematyczny rocznych planów współpracy MON z organizacjami pozarządowymi, kładąc większy nacisk (i przeznaczając proporcjonalnie większe środki) na przedsięwzięcia o największym znaczeniu dla wzmacniania strategicznej odporności kraju na ewentualną agresję.
11. Zwiększenie zaangażowania NGO we wzmacnianie strategicznej odporności kraju – nie może oznaczać tworzenia „wojska poza wojskiem". Lokalny charakter potrzeb pozostaje w sprzeczności z ambicjami niektórych NGO, zamierzających tworzyć struktury ogólnokrajowe.
12. Doskonałą okazją do promowania Katalogu Potrzeb i Możliwości będzie Kongres NGO planowany przez Pełnomocnika Ministra Obrony Narodowej ds. Społecznych Inicjatyw Proobronnych w I kwartale 2015 r.

Podsumowanie:

- Projekt Katalogu Potrzeb i Możliwości opracowany w BBN – jest kompilacją propozycji i sugestii zebranych w ramach przeprowadzonej kwerendy oraz prac własnych Biura. Nie ma charakteru zamkniętego (skończonego), proponuje jedynie sposób uporządkowania obszaru współpracy państwa z organizacjami pozarządowymi we wzmacnianiu strategicznej odporności kraju. Aktualną wersję Katalogu należy traktować jako punkt wyjścia do dalszych prac.
- Na obecnym etapie Katalog uwzględnia w większym stopniu potrzeby strony „rządowej" (obszary i zadania dla NGO). Przyporządkowanie poszczególnych organizacji ma charakter jedynie poglądowy – bazuje na ich zadaniach statutowych – i wymaga stosownych korekt.
- W dalszych pracach należy sformalizować kategorie zadań i rozszerzyć Katalog o informacje ilościowe i jakościowe dotyczące zarówno potrzeb, jak i zdolności/możliwości deklarowanych przez organizacje. Ta rozszerzona wersja Katalogu umożliwi przejście od planowania do programowania (zaplanowanie stosownych środków finansowych).
- W miarę postępu prac należy uwzględniać pojawianie się elementów wymagających zachowania zasad poufności, dyktowanych względami bezpieczeństwa państwa.
- Rozszerzaniu form zaangażowania NGO we wzmacnianie strategicznej odporności kraju na ewentualną agresję powinny od początku towarzyszyć mechanizmy kontrolne, umożliwiające weryfikację skuteczności i celowości podejmowanych działań oraz kontrolę wydatków.

4 lutego 2015 r.

REKOMENDACJE BBN WS. ROLI ORGANIZACJI POZARZĄDOWYCH WE WZMACNIANIU STRATEGICZNEJ ODPORNOŚCI KRAJU

KATALOG POTRZEB I MOŻLIWOŚCI

CZAS POKOJU

LP	ORGANY I INSTYTUCJE PAŃSTWOWE (zainteresowane lub wg właściwości) (POTRZEBY)	ZDOLNOŚCI WZMACNIAJĄCE (obronne, szkoleniowe, ratownicze, inne)		ORGANIZACJE DYSPONUJĄCE STOSOWNYM POTENCJAŁEM (MOŻLIWOŚCI)	UWAGI
		OBSZAR (DZIEDZINA) WZMOCNIENIA	ZADANIA		
1.	MON MSW (Policja) MAiC MEN Terenowe organy władzy oraz samorządu terytorialnego	Obronność[3]	a) przygotowanie specjalistów na potrzeby sił zbrojnych b) doskonalenie rezerwistów c) prowadzenie szkolenia obronnego w zakresie technicznym, strzeleckim i ratowniczym d) popularyzowanie roli i zadań wojska, jego tradycji oraz wzmacnianie więzi z narodem e) ochrona porządku publicznego	• Organizacje paramilitarne (np. Związek Strzelecki "Strzelec" - OSW, Fidelis et Instructi Armi - FIA, ObronaNarodowa.pl, etc) • Organizacje harcerskie (ZHP, ZHR) • Ruch Obywatelski Miłośników Broni (ROMB) • Towarzystwo Wiedzy Obronnej • Ruch Wspólnot Obronnych • Liga Obrony Kraju • Legia Akademicka • Związek Polskich Spadochroniarzy • Karate Combat • Inne	Zgodnie z zadaniami statutowymi organizacji
2.	Terenowe organy władzy oraz samorządu terytorialnego MSW MAiC Państwowa Straż Pożarna, Policja, Straż Graniczna,	Przeciwdziałanie klęskom żywiołowym[4]	a) wykrywanie, ostrzeganie i alarmowanie b) przygotowanie oraz udział w udzielaniu pomocy poszkodowanym w wyniku klęsk i katastrof	• Organizacje paramilitarne (np. Związek Strzelecki "Strzelec" - OSW, Fidelis et Instructi Armi - FIA, ObronaNarodowa.pl), etc. • Organizacje harcerskie (ZHP, ZHR)	

[3] Konstytucja RP, Ustawa z 21.11.1967 r. *o powszechnym obowiązku obrony RP*
[4] Ustawa z 18.04.2002 r. *O stanie klęski żywiołowej*

	Morska Służba Poszukiwania i Ratownictwa, Państwowe Ratownictwo Medyczne			• Organizacje ratownicze: WOPR, GOPR • Ochotnicze Straże Pożarne • Inne	
3.	Min. Zdrowia MEN Państwowa Straż Pożarna MSW MON Terenowe organy władzy oraz samorządu terytorialnego	Wsparcie ochrony i obrony ludności, ratownictwo medyczne[5]	a) Wsparcie zabezpieczenia bytowego ludności (zbiórki, magazynowanie i dystrybucja lekarstw, wody i żywności) b) realizacja szkoleń z zakresu ratownictwa medycznego, pierwsza pomoc przedmedyczna c) Ewakuacja poszkodowanych (zagrożonych) ludzi, zwierząt i mienia	• Federacja Polskich Banków Żywności • Polski Czerwony Krzyż • Organizacje paramilitarne (np. Związek Strzelecki "Strzelec" - OSW, Fidelis et Instructi Armi - FIA, ObronaNarodowa.pl) • Organizacje harcerskie (ZHP, ZHR) • Organizacje ratownicze: WOPR, GOPR • Inne	
4.	MEN MNiSW MON	Edukacja obywatelska i przysposobienie obronne	a) Szkolenie ogniowe i taktyczne, pierwsza pomoc, ratownictwo pola walki, kursy i szkolenia (np. Combat Lifesaver) b) Wychowanie patriotyczne, edukacja historyczna c) Promocja obronności i wojskowości	• Związek Strzelecki "Strzelec" - OSW • Fidelis et Instructi Armi - FIA • ObronaNarodowa.pl • Ruch Obywatelski Miłośników Broni (ROMB) • Towarzystwo Wiedzy Obronnej • Ruch Wspólnot Obronnych • Liga Obrony Kraju • Legia Akademicka • Związek Polskich Spadochroniarzy	Ujednolicone wymagania, plany szkolenia oraz certyfikaty, potwierdzające uzyskane kwalifikacje
5.	MAiC MSZ MSW MON Min. Infrastruktury	Zapewnienie komunikacji ze społeczeństwem i wymiany informacji, bieżące informowanie i powiadamianie społeczeństwa	a) Szkolenia techniczne - obsługa sprzętu łączności b) Wspieranie tworzenia i utrzymywania dodatkowych sieci łączności dla władz lokalnych c) Popularyzacja wiedzy i umiejętności posługiwania się sprzętem łączności (kursy, szkolenia, etc.) d) Udział w programach informacyjnych (media elektroniczne, środki masowego przekazu) e) Internet: prowadzenie tematycznych portali, aktywność na forach społecznościowych	• Polski Związek Krótkofalowców • Pozostałe organizacje - zgodnie z zadaniami statutowymi	
6.	MSW Min. Kultury i Dziedzictwa Narodowego Terenowe organy władzy oraz samorządu terytorialnego Szef Obrony Cywilnej Kraju	Ochrona dóbr kultury[6]	a) Wsparcie katalogowania dóbr kultury i przygotowania ukryć dla dóbr kultury na czas "K" i "W" b) Wspieranie przygotowania akcji zabezpieczenia dóbr kultury na czas "P" i "W"	• Organizacje akademickie • Towarzystwo Wiedzy Obronnej • Inne	
7.	Min. Infrastruktury MSW MAiC MON Terenowe organy władzy oraz samorządu	Przygotowanie i utrzymanie infrastruktury ochronnej i obronnej	a) Pomoc w zapewnieniu przejezdności dróg b) Osłona techniczna infrastruktury drogowej c) Wspieranie przygotowania, utrzymywania i konserwacji schronów i umocnień d) Uczestniczenie w przygotowaniu	• Ochotnicze Straże Pożarne • Organizacje proobronne oraz inne - zgodnie z regulacjami statutowymi	

[5] Ustawa z 8.09.2006 r. *o Państwowym Ratownictwie Medycznym*

[6] Ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami

	terytorialnego Szef Obrony Cywilnej Kraju		lokalnych planów ochrony infrastruktury krytycznej e) Rozpoznawanie potrzeb i możliwości zabezpieczenia dostępu do wody pitnej		
8.	Min. Środowiska Min. Gospodarki	Ochrona środowiska[7]	a) Monitoring b) podjęcie lub zaniechanie działań umożliwiających zachowanie lub przywrócenie równowagi przyrodniczej	• Ochotnicze Straże Pożarne • Inne organizacje proobronne - zgodnie z regulacjami statutowymi	

CZAS KRYZYSU

LP	ORGANY I INSTYTUCJE PAŃSTWOWE (zainteresowane lub wg właściwości) (POTRZEBY)	ZDOLNOŚCI WZMACNIAJĄCE (obronne, szkoleniowe, ratownicze, inne)		ORGANIZACJE DYSPONUJĄCE STOSOWNYM POTENCJAŁEM (MOŻLIWOŚCI)	UWAGI
		OBSZAR (DZIEDZINA) WZMOCNIENIA	POTRZEBY I ZADANIA		
1.	Min. Gospodarki MON, MSW, MAiC Min. Zdrowia Min. Infrastruktury Państwowa Straż Pożarna Terenowe organy władzy oraz samorządu terytorialnego **Szef Obrony Cywilnej Kraju**	Polityczno-militarny - wsparcie bytowe ludności	a) Wsparcie zabezpieczenia bytowego ludności (zbiórki, magazynowanie i dystrybucja lekarstw, wody i żywności) - w czasie klęsk żywiołowych i awarii technicznych o dużej skali b) niesienie pomocy humanitarnej - udzielanie pomocy ludności w trudnej sytuacji	• Federacja Polskich Banków Żywności • Polski Czerwony Krzyż • organizacje paramilitarne, ratownicze, straże, itd.	Zgodnie z lokalnymi planami reagowania kryzysowego
2.	MSW, MON Państwowa Straż Pożarna Policja **Szef Obrony Cywilnej Kraju** Min. Zdrowia MEN Terenowe organy władzy oraz samorządu terytorialnego	Wsparcie w ochronie i obronie ludności	a) udział w likwidacji skutków zakłóceń porządku publicznego, działania terrorystycznego, katastrofy naturalnej i awarii technicznej, których skutki zagrażają konstytucyjnemu ustrojowi państwa, bezpieczeństwu obywateli, życiu lub zdrowiu dużej liczby ludzi, mieniu w wielkich rozmiarach albo środowisku na znacznym obszarze. b) Ratownictwo, pierwsza pomoc przedmedyczna c) Ewakuacja poszkodowanych (zagrożonych) ludzi, zwierząt i mienia d) Oznakowanie i zabezpieczenie miejsc prowadzenia działań ratowniczych e) pomoc w utrzymaniu porządku publicznego	• Federacja Polskich Banków Żywności • Polski Czerwony Krzyż • Organizacje paramilitarne (np. Związek Strzelecki "Strzelec" - OSW, Fidelis et Instructi Armi - FIA, ObronaNarodowa.pl) • Organizacje harcerskie (ZHP, ZHR) • Organizacje ratownicze: WOPR, GOPR • Ochotnicze Straże Pożarne • Straże miejskie i gminne	Zgodnie z lokalnymi planami reagowania kryzysowego
3.	MEN MNiSW MON MSW	Edukacja obywatelska i przysposobienie obronne	a) Szkolenie i praktyczne wspieranie udzielania pierwszej pomocy b) Szkolenie w zakresie zachowania w sytuacjach kryzysowych c) Szkolenie ogniowe i taktyczne, ratownictwo pola walki, kursy i szkolenia (np. Combat Lifesaver) - zgrywanie i doskonalenie umiejętności d) Wychowanie patriotyczne, edukacja historyczna e) Promocja obronności i wojskowości	• Związek Strzelecki "Strzelec" - OSW • Fidelis et Instructi Armi - FIA • ObronaNarodowa.pl • Ruch Obywatelski Miłośników Broni (ROMB) • Towarzystwo Wiedzy Obronnej • Ruch Wspólnot Obronnych • Liga Obrony Kraju	

[7] Ustawa z 27.04.2001 r. *Prawo Ochrony środowiska*

				• Legia Akademicka • Związek Polskich Spadochroniarzy • Karate Combat	
4.	MAiC Min. Infrastruktury MON MSW MSZ	Zapewnienie komunikacji ze społeczeństwem i wymiany informacji, bieżące informowanie i powiadamianie społeczeństwa	a) Wsparcia dla władz lokalnych w utrzymywaniu łączności (wprowadzenie dyżurów, wsparcie - w zależności od potrzeb - systemu powiadamiania i informowania b) Szkolenia techniczne - obsługa sprzętu łączności	• Polski Związek Krótkofalowców • Organizacje harcerskie (ZHP, ZHR) • Inne	
5.	MSW Min. Kultury i Dziedzictwa Narodowego Terenowe organy władzy oraz samorządu terytorialnego Szef Obrony Cywilnej Kraju	Ochrona dóbr kultury	a) Wzmocnienie zabezpieczenia dóbr kultury b) Pomoc w przeprowadzaniu akcji zabezpieczenia dóbr kultury	• Organizacje akademickie • Towarzystwo Wiedzy Obronnej • Inne	
6.	Min. Infrastruktury MSW MAiC MON Terenowe organy władzy oraz samorządu terytorialnego Szef Obrony Cywilnej Kraju	Przygotowanie i utrzymanie infrastruktury ochronnej i obronnej	a) Pomoc w likwidacji skutków klęsk żywiołowych b) Utrzymanie rejonów ewakuacji ludności c) Pomoc w zapewnieniu przejezdności dróg d) Osłona techniczna infrastruktury drogowej e) Wsparcie w kierowaniu ruchem f) Zapewnienie dostępu do wody pitnej	• Ochotnicze Straże Pożarne • ZS "Strzelec" OSW, • FIA • Związek Harcerstwa Polskiego	
7.	Min. Środowiska Min. Gospodarki Min. Infrastruktury MAiC MSW (PSP, Policja) MON	Ochrona środowiska	a) Podejmowanie działań umożliwiających ochronę i zachowanie środowiska naturalnego b) Usuwanie skutków katastrof grożących degradacją środowiska c) Przywracanie równowagi przyrodniczej	• Ochotnicze Straże Pożarne • Pozostałe NGO – zgodnie z regulacjami statutowymi	

CZAS WOJNY

LP	ORGANY I INSTYTUCJE PAŃSTWOWE (zainteresowane lub wg właściwości) (POTRZEBY)	ZDOLNOŚCI WZMACNIAJĄCE (obronne, szkoleniowe, ratownicze, inne)		ORGANIZACJE DYSPONUJĄCE STOSOWNYM POTENCJAŁEM (MOŻLIWOŚCI)	UWAGI
		OBSZAR (DZIEDZINA) WZMOCNIENIA	POTRZEBY I ZADANIA		
1.	MON MSW (Policja, PSP) Szef Obrony Cywilnej Terenowe organy władzy oraz samorządu terytorialnego MAiC MEN Ministerstwa: Infrastruktury, Gospodarki, Skarbu, Finansów	Stan wojenny: a) wsparcie ochrony i obrony narodowej b) wsparcie na rzecz zapewnienia swobody operacyjnej w Strefie Działań Bezpośrednich (SDB) c) wsparcie działań niekinetycznych w SDB	a) Stworzenie niezbędnych warunków do funkcjonowania Sił Zbrojnych RP, poprzez zapewnienie ochrony ludności i struktur państwa w sytuacji zagrożenia bezpieczeństwa narodowego i wojny b) uzupełnianie zasobów osobowych dla poddziałów Obrony Terytorialnej oraz Narodowych Sił Rezerwowych (indywidualne lub zespołowe) c) zasilanie Sił Zbrojnych RP zasobami ludzkimi i materiałowymi d) wsparcie wojsk sojuszniczych prowadzących operacje na terytorium RP e) utrzymanie materialnych i duchowych podstaw egzystencji	• Organizacje paramilitarne (np. Związek Strzelecki "Strzelec" - OSW, Fidelis et Instructi Armi - FIA, ObronaNarodowa.pl) • Organizacje harcerskie (ZHP, ZHR) • Towarzystwo Wiedzy Obronnej • Ruch Wspólnot Obronnych • Liga Obrony Kraju • Legia Akademicka • Inne	Wsparcie ochrony i obrony narodowej zgodnie z *Ustawą o powszechnym obowiązku obrony RP*

			ludności w czasie wojny f) Wsparcie ochrony mienia i środowiska g) Wsparcie organów władzy i instytucji państwowych h) Zapobieganie grabieżom oraz niszczeniu mienia i zapasów i) Wsparcie ewakuacji ludności j) Wsparcie utrzymania porządku publicznego		
2.	MON MSW (Policja, PSP) Szef Obrony Cywilnej Terenowe organy władzy oraz samorządu terytorialnego MAiC Min. Infra-struktury, Min. Gospodarki	Przygotowanie rejonów obrony, rozbudowa inżynieryjna w SDB	a) Wsparcie przygotowania zaplecza dla wojsk (infrastruktura, fortyfikacje ziemne, pomieszczenia, schrony, ukrycia) b) Wsparcie rozbudowy inżynieryjnej	• Ochotnicze Straże Pożarne • Związek Strzelecki "Strzelec" - OSW • Fidelis et Instructi Armi - FIA • ObronaNarodowa.pl	
3.	MON MSW (Policja, PSP) Szef Obrony Cywilnej Terenowe organy władzy oraz samorządu terytorialnego MAiC	Mobilizacja, rozwinięcie i wsparcie działań wojsk	a) Wsparcie akcji mobilizacyjnej, akcji kurierskich i powiadamiania ludności b) usprawnienie świadczeń osobistych i rzeczowych ludności na rzecz Sił Zbrojnych RP	• Organizacje paramilitarne (np. Związek Strzelecki "Strzelec" - OSW, Fidelis et Instructi Armi - FIA, ObronaNarodowa.pl) • Polski Związek Krótkofalowców • Organizacje harcerskie (ZHP, ZHR) • Inne	
4.	Szef Obrony Cywilnej Terenowe organy władzy oraz samorządu terytorialnego MSW (Policja, PSP)	Inne zadania w ramach powszechnego obowiązku obrony - przygotowanie ludności do obrony	a) organizacja samoobrony ludności i ochrony obiektów, lokalne patrole samoobrony mieszkańców b) obsługa środków zaciemnienia, wykrywanie i oznaczanie stref niebezpiecznych, odkażanie sprzętu c) Formowanie ochotniczych formacji obronnych d) Obsługa broni, taktyka - szkolenie, treningi, doskonalenie umiejętności e) Rozpoznanie i likwidacja grup dywersyjnych f) wsparcie w walce z pożarami g) pomoc w usuwaniu skutków zniszczeń infrastruktury specjalistycznej wojska h) Szkolenie i prowadzenie działań nieregularnych na terenach czasowo zajętych przez agresora i) Doskonalenie (szkolenie) i praktyczne udzielanie pierwszej pomocy oraz ratownictwo pola walki j) Pomoc w kształtowaniu postaw społecznych i utrzymaniu wysokiego morale	• Związek Strzelecki "Strzelec" - OSW • Fidelis et Instructi Armi - FIA • ObronaNarodowa.pl • Ruch Obywatelski Miłośników Broni (ROMB) • Towarzystwo Wiedzy Obronnej • Ruch Wspólnot Obronnych • Liga Obrony Kraju • Legia Akademicka • Związek Polskich Spadochroniarzy • Karate Combat • Ochotnicze Straże Pożarne	Zgodnie ze specyfiką, zdolnościami i potencjałem organizacji pozarządowych.
5.	Min. Gospodarki Min. Infrastruktury Min. Zdrowia Szef Obrony Cywilnej Terenowe organy władzy oraz samorządu terytorialnego MSW (Policja, PSP)	Wsparcie w ochronie i obronie ludności	a) Wsparcie zabezpieczenia bytowego ludności (zbiórki, magazynowanie i dystrybucja lekarstw, wody i żywności) b) Ratownictwo, pierwsza pomoc przedmedyczna c) Ewakuacja poszkodowanych (zagrożonych) ludzi, zwierząt i mienia	• Federacja Polskich Banków Żywności • Polski Czerwony Krzyż • Organizacje paramilitarne (np. Związek Strzelecki "Strzelec" - OSW, Fidelis et Instructi Armi - FIA, ObronaNarodowa.pl) • Organizacje harcerskie (ZHP, ZHR) • Organizacje ratownicze: WOPR, GOPR	
6.	Szef Obrony	Zapewnienie	a) Wsparcia w utrzymywaniu łączności	• Polski Związek	

	Cywilnej Min. Infrastruktury Terenowe organy władzy oraz samorządu terytorialnego MSW (Policja, PSP)	komunikacji ze społeczeństwem i wymiany informacji, bieżące informowanie i powiadamianie społeczeństwa	dla władz lokalnych (wprowadzenie dyżurów, wsparcie - w zależności od potrzeb - systemu powiadamiania i informowania b) Szkolenia techniczne - obsługa sprzętu łączności	Krótkofalowców • Organizacje harcerskie (ZHP, ZHR) • inne - w zależności od możliwości i potrzeb	
7.	Min. Kultury i Dziedzictwa Narodowego Terenowe organy władzy oraz samorządu terytorialnego Szef Obrony Cywilnej Kraju	Ochrona dóbr kultury	a) Pomoc w ewakuacji i ukryciu dóbr kultury	• Organizacje akademickie • Towarzystwo Wiedzy Obronnej • Inne	
8.	MSW MON Min. Infrastruktury Min. Gospodarki MAiC Terenowe organy władzy oraz samorządu terytorialnego Szef Obrony Cywilnej Kraju	Wsparcie utrzymania infrastruktury ochronnej i obronnej	a) Utrzymanie rejonów ewakuacji ludności b) Pomoc w zapewnieniu przejezdności dróg c) Wsparcie ochrony infrastruktury drogowej d) Wsparcie w kierowaniu ruchem (cywilnym i wojskowym) e) Wsparcie organizacji dostępu do wody pitnej	• Ochotnicze Straże Pożarne • Organizacje paramilitarne (ZS "Strzelec" OSW, FIA, inne) • Związek Harcerstwa Polskiego	

DOKTRYNA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ

Dokument przygotowany został w Biurze Bezpieczeństwa Narodowego po przeprowadzeniu analiz z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego. Jego założenia zostały rozpatrzone i zaakceptowane przez Radę Bezpieczeństwa Narodowego 12 stycznia 2015 r.

Celem Doktryny – jako dokumentu o charakterze wykonawczym do Strategii Bezpieczeństwa Narodowego RP – jest wskazanie kierunków działań dla zapewnienia bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Jednocześnie Doktryna powinna być traktowana jako wspólny mianownik działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny oraz obywateli.

Doktryna została opublikowana 22 stycznia 2015 r.

BIURO BEZPIECZEŃSTWA NARODOWEGO

22 stycznia 2015 r.

DOKTRYNA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ

SŁOWO WSTĘPNE
PREZYDENTA RZECZYPOSPOLITEJ POLSKIEJ

Szanowni Państwo,

Jedną z najważniejszych zmian we współczesnym środowisku bezpieczeństwa jest pojawienie się nowego obszaru aktywności państwa, podmiotów prywatnych i obywateli, jakim jest cyberprzestrzeń. Zmiana ta sprawia, że musimy być przygotowani na zagrożenia z jakimi wcześniej nie mieliśmy do czynienia.

Cyberprzestrzeń jest polem konfliktu, na którym przychodzi nam zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi, czy zorganizowanymi grupami przestępczymi. Dlatego jednym z istotnych priorytetów polskiej strategii stało się bezpieczeństwo tego nowego środowiska.

Zgodnie z tym priorytetem dokonaliśmy już pewnych zmian w polskim systemie prawnym, wprowadzając do niego w 2011 r. m.in. pojęcie cyberprzestrzeni oraz ustanawiając prawne podstawy nadzwyczajnego reagowania na występujące w niej zagrożenia. W pełni wykorzystujemy dorobek Unii Europejskiej i NATO w tej dziedzinie. Na potrzeby polskiej administracji wprowadzono nowe rozwiązania w toku prac nad Polityką Ochrony Cyberprzestrzeni RP, przyjętą przez Radę Ministrów w 2013 r. Dokument ten dotyczy przede wszystkim ochrony cyberprzestrzeni w wymiarze pozamilitarnym. W Ministerstwie Obrony Narodowej trwają prace nad budową systemu cyberobrony. Prywatne podmioty dbają o swoje bezpieczeństwo w cyberprzestrzeni także we własnym zakresie.

Celem niniejszej doktryny jest stworzenie warunków do połączenia i strategicznego ukierunkowania tych wysiłków na rzecz budowania zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Dokument przygotowany został w wyniku analiz prowadzonych z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego. Główne założenia doktryny zostały rozpatrzone i zaakceptowane przez Radę Bezpieczeństwa Narodowego.

Doktryna cyberbezpieczeństwa wskazuje strategiczne kierunki działań dla zapewnienia bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Jednocześnie powinna być traktowana jako jednolita podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony – jako wspólny mianownik dla działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny oraz obywateli. Dzięki temu doktryna cyberbezpieczeństwa może stanowić punkt wyjścia do dalszych prac na rzecz wzmocnienia bezpieczeństwa Polski.

Bronisław Komorowski

22 stycznia 2015 r.

DOKTRYNA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ

WPROWADZENIE

1. We współczesnym świecie bezpieczeństwo państwa – zarówno w sferze militarnej, jak i pozamilitarnej – zyskało dodatkowy wymiar, jakim – obok lądu, wody, powietrza i przestrzeni kosmicznej – jest cyberprzestrzeń.

2. Działania na rzecz cyberbezpieczeństwa i wszelkie zadania realizowane w tym zakresie muszą być podejmowane z uwzględnieniem zasad ochrony praw człowieka i obywatela, z zachowaniem poszanowania prawa do wolności słowa i prywatności. Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnych i wiarygodnych mechanizmach analizy ryzyka.

3. Bazę wyjściową niniejszej Doktryny stanowią kierunkowe postanowienia Strategii Bezpieczeństwa Narodowego dotyczące cyberbezpieczeństwa RP, a także ustalenia Polityki Ochrony Cyberprzestrzeni RP oraz Strategii bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń.

4. Główne kategorie pojęciowe przyjęte w niniejszej Doktrynie:

   - **cyberprzestrzeń –** przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami;
   - **cyberprzestrzeń RP** – cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji);
   - **cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni)** – proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni;
   - **bezpieczeństwo cyberprzestrzeni RP** – część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych;

- **środowisko cyberbezpieczeństwa –** ogół warunków funkcjonowania danego podmiotu w cyberprzestrzeni charakteryzowany przez wyzwania (szanse i ryzyka) oraz zagrożenia dla osiągania przyjętych celów;
- **wyzwania cyberbezpieczeństwa –** sytuacje problemowe w dziedzinie cyberbezpieczeństwa, stwarzane zwłaszcza przez szanse i ryzyka oraz generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw cyberbezpieczeństwa;
- **szanse cyberbezpieczeństwa –** niezależne od woli podmiotu okoliczności (zjawiska i procesy w środowisku bezpieczeństwa) sprzyjające realizacji interesów oraz osiąganiu celów podmiotu w dziedzinie cyberbezpieczeństwa;
- **ryzyka cyberbezpieczeństwa –** możliwości negatywnych dla danego podmiotu skutków własnego działania w sferze cyberbezpieczeństwa;
- **zagrożenia cyberbezpieczeństwa –** pośrednie lub bezpośrednie zakłócające lub destrukcyjne oddziaływania na podmiot w cyberprzestrzeni;
- **Doktryna cyberbezpieczeństwa RP –** oficjalne poglądy i ustalenia dotyczące celów, ocen środowiska oraz koncepcji (zasad i sposobów) działania (w tym tzw. dobrych praktyk) dla zapewnienia bezpiecznego funkcjonowania państwa jako całości, jego struktur, osób fizycznych i osób prawnych – w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej – w cyberprzestrzeni.

1. CELE STRATEGICZNE RP W DZIEDZINIE CYBERBEZPIECZEŃSTWA

5. **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.

6. Cel strategiczny osiąga się przez realizację celów o charakterze **operacyjnym i preparacyjnym.** Do najważniejszych celów operacyjnych prowadzących do zapewnienia cyberbezpieczeństwa należą:
   - ocena warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie ryzyk i identyfikacja szans;
   - zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie ryzyk i wykorzystywanie szans;
   - obrona i ochrona własnych systemów i zgromadzonych w nich zasobów;
   - zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne);
   - po ewentualnym ataku – odtwarzanie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń.

7. Dla osiągnięcia tych celów potrzebne jest, w **wymiarze preparacyjnym,** zbudowanie zintegrowanego, zarządzanego (koordynowanego), ponadresortowo, systemu cyberbezpieczeństwa RP obejmującego podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie cyberbezpieczeństwa – oraz podsystemy operacyjne i wsparcia, zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych

cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach kolektywnych działań sojuszniczych.

2 . ŚRODOWISKO CYBERBEZPIECZEŃSTWA RP

2.1. WYMIAR WEWNĘTRZNY

2.1.1 Zagrożenia

8. Wraz z postępującym rozwojem technologicznym wewnętrzne zagrożenia bezpieczeństwa wewnętrznego, należące do katalogu form tradycyjnych, na coraz większą skalę znajdować mogą swoje odpowiedniki (analogie) w cyberprzestrzeni. Zarówno cyberprzestępczość, cyberprzemoc (tzw. *cyberbullying*), cyberprotesty i cyberdemonstracje o charakterze destrukcyjnym, zakłócające realizowanie istotnych zadań administracji publicznej oraz sektora prywatnego – to zjawiska, które są już obecne w przestrzeni wirtualnej.

9. Wśród cyberzagrożeń szczególnie istotne są zagrożenia dla infrastruktury krytycznej państwa sterowanej za pomocą systemów informatycznych. W tym obszarze kluczowe znaczenie mogą mieć celowe ataki lub wadliwe procedury w obszarze komunikacji w podsystemie kierowania bezpieczeństwem narodowym, komunikacji w podsystemie obronnym i podsystemach ochronnych oraz w podsystemach wsparcia (gospodarczym i społecznym).

10. Funkcjonowanie w cyberprzestrzeni nie ogranicza się jedynie do podmiotów publicznych. W tej samej przestrzeni współistnieją i współdziałają z państwem podmioty sektora prywatnego oraz obywatele. Zwłaszcza podmioty sektora prywatnego – szczególnie te należące do sektora finansowego, energetycznego, transportowego, zdrowia publicznego – zagrożone są zjawiskami takimi, jak kradzież danych lub naruszenie ich integralności albo naruszenie poufności prowadzonych działań, a także naruszenie dostępności usług.

11. Na zagrożenia narażeni są także operatorzy oraz dostawcy usług telekomunikacyjnych i teleinformatycznych. Zakłócenia ich działalności, szczególnie przerwanie ciągłości świadczenia usług, przekładać się mogą na zakłócenia funkcjonowania instytucji państwowych, jak również podmiotów sektora prywatnego i obywateli w cyberprzestrzeni.

12. Odrębną kategorią zagrożeń są zjawiska, z którymi stykają się obywatele RP. W dobie przenoszenia do cyberprzestrzeni wielu usług świadczonych przez administrację publiczną oraz usług o charakterze finansowym, poważnym zagrożeniem stają się kradzieże danych, kradzieże tożsamości i przejmowanie kontroli nad prywatnymi komputerami.

2.1.2 Wyzwania (ryzyka i szanse)

13. Ryzyka w dziedzinie cyberbezpieczeństwa RP wiążą się z istniejącymi lukami w systemie cyberbezpieczeństwa. Do ich najbardziej dolegliwych źródeł zaliczyć można nieuregulowane lub niewłaściwie uregulowane relacje między poszczególnymi podmiotami w tym systemie (co może wynikać z niedostatków w zakresie komunikacji i wymiany informacji, a także z braku precyzji w określeniu zakresu odpowiedzialności w odniesieniu do przeciwdziałania cyberzagrożeniom) oraz luki prawne, np. w zakresie obowiązku raportowania o wystąpieniu istotnych incydentów bezpieczeństwa w systemach teleinformatycznych, a także obowiązku współpracy przy próbie ich rozwiązania z powołanymi do tego zespołami.

14. Ryzyka w dziedzinie cyberbezpieczeństwa potęgowane są przez dynamikę coraz większego wykorzystywania przez instytucje publiczne zaawansowanych systemów informatycznych do wykonywania zadań o krytycznym znaczeniu dla funkcjonowania społeczeństwa.

15. Wyjątkowo poważne ryzyka wiążą się z wykorzystaniem na potrzeby bezpieczeństwa narodowego (militarnego, pozamilitarnego, zewnętrznego i wewnętrznego) wysoce zinformatyzowanych systemów technicznych obcej produkcji, zwłaszcza systemów walki i wsparcia (w szczególności zautomatyzowanych systemów dowodzenia i kierowania), bez uzyskania gwarancji informatycznego panowania nad nimi.

16. Istotnym ryzykiem pozostaje potencjalne ograniczenie dostępności, integralności i poufności danych przetwarzanych w systemach teleinformatycznych administracji publicznej oraz brak skutecznych zabezpieczeń teleinformatycznych i planów przywracania prawidłowego funkcjonowania systemów.

17. Źródłem ryzyk może być nieodpowiedni poziom finansowania zespołów powołanych do koordynacji reagowania na incydenty komputerowe na poziomie krajowym, a także przeznaczanie niedostatecznych środków finansowych na wdrożenia mechanizmów zabezpieczających dedykowanych eksploatowanym systemom teleinformatycznym.

18. Ryzyka dla cyberbezpieczeństwa RP mogą wynikać także ze struktury własności podmiotów prywatnych będących operatorami i dostawcami usług teleinformatycznych, szczególnie w wypadku podmiotów transnarodowych o ponadpaństwowych ośrodkach decyzyjnych, co powoduje, że państwo ma na nie ograniczony wpływ.

19. Do działań obarczonych ryzykiem, zwłaszcza z punktu widzenia podmiotów gospodarczych oraz obywateli, zaliczyć należy wprowadzanie zmian organizacyjnych i regulacyjnych, będących następstwem budowania systemu cyberbezpieczeństwa, bez dialogu i konsultacji społecznych, co może powodować sprzeciw społeczny motywowany obawami dotyczącymi ewentualnych naruszeń praw człowieka czy wolności gospodarczej.

20. Coraz szersze zagospodarowanie cyberprzestrzeni może stwarzać ryzyko braku akceptacji społecznej dla racjonalnego określenia granicy między wolnością osobistą i ochroną praw jednostki w świecie wirtualnym a stosowaniem środków służących zapewnieniu akceptowalnego poziomu bezpieczeństwa, co może powodować trudności we wprowadzaniu nowych, efektywnych systemów bezpieczeństwa w cyberprzestrzeni.

21. Szanse w dziedzinie cyberbezpieczeństwa stwarza potencjał naukowy RP w dziedzinie nauk informatycznych i matematycznych, dający możliwość rozwijania narodowych systemów służących cyberbezpieczeństwu oraz kryptologii, w tym kryptografii, zapewniających suwerenne panowanie nad systemami teleinformatycznymi należącymi do państwa.

22. Jako szansę należy wskazać także rosnącą świadomość w zakresie cyberbezpieczeństwa (zarówno wśród obywateli, jak i prywatnych podmiotów, które coraz częściej pozytywnie odnoszą się do współpracy z państwem).

2.2. WYMIAR ZEWNĘTRZNY

2.2.1 Zagrożenia

23. Pojawienie się nowych technologii teleinformatycznych oraz rozwój sieci internetowej prowadzą do powstawania nowych zagrożeń zewnętrznych takich jak cyberkryzysy i cyberkonflikty z udziałem podmiotów państwowych i niepaństwowych, w tym cyberwojny. Operacje w cyberprzestrzeni są już dziś integralną częścią klasycznych

kryzysów i konfliktów polityczno-militarnych (wojen), w ramach ich hybrydowego charakteru.

24. Poważnym zagrożeniem zewnętrznym w cyberprzestrzeni jest cyberszpiegostwo, związane z wykorzystywaniem specjalistycznych narzędzi i długofalowych, precyzyjnie wymierzonych działań zmierzających do uzyskania – zarówno przez służby nieprzyjaźnie nastawionych państw, jak też organizacje terrorystyczne – dostępu do danych newralgicznych z punktu widzenia działania struktur państwa.

25. Źródłami zagrożeń w cyberprzestrzeni są także organizacje ekstremistyczne, terrorystyczne oraz zorganizowane transnarodowe grupy przestępcze, których ataki w cyberprzestrzeni mogą mieć podłoże ideologiczne, polityczne, religijne, biznesowe i kryminalne.

2.2.2 Wyzwania (ryzyka i szanse)

26. Ryzyka generować może, szczególnie w ramach współpracy z partnerami międzynarodowymi i sojusznikami, nieodpowiednie określenie, a zwłaszcza brak wspólnie przyjętych definicji prawnych (kategorii pojęciowych) nowych zjawisk i procesów w cyberprzestrzeni oraz zadań i działań realizowanych przez systemy bezpieczeństwa narodowego i międzynarodowego w celu zapewnienia cyberbezpieczeństwa. Dotyczy to szczególnie kategorii cyberkonfliktu i cyberwojny.

27. Szansą dla wzmocnienia cyberbezpieczeństwa RP jest możliwość wykorzystania członkostwa Polski w sojuszniczych strukturach obrony cybernetycznej (NATO, UE) oraz aktywny i ukierunkowany na potrzeby państwa udział w pracach organizacji międzynarodowych oraz aktywność na forum międzynarodowych gremiów zajmujących się bezpieczeństwem w cyberprzestrzeni, a także bilateralna współpraca z państwami bardziej zaawansowanymi w sprawach cyberbezpieczeństwa.

3. KONCEPCJA ZADAŃ OPERACYJNYCH W DZIEDZINIE CYBERBEZPIECZEŃSTWA

28. Zadania operacyjne ukierunkowane na osiągnięcie strategicznego celu, jakim jest zapewnienie akceptowalnego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni, powinny być realizowane przez podmioty sektora publicznego (na poziomie krajowym i międzynarodowym), prywatnego (komercyjnego), obywatelskiego oraz w wymiarze transsektorowym.

29. Do głównych zadań w sektorze publicznym na poziomie krajowym należą:

- rozpoznawanie realnych i potencjalnych źródeł zagrożeń, w tym przez wymianę informacji na arenie międzynarodowej;
- prowadzenie regularnej analizy ryzyka w odniesieniu do ważnych obiektów infrastruktury krytycznej, również tej służącej zadaniom NATO i UE;
- realizacja działań w dziedzinie kryptografii i kryptoanalizy na potrzeby zabezpieczenia własnych zasobów informacyjnych oraz rozpoznania potencjalnych zagrożeń ze strony wrogich państw i podmiotów niepaństwowych;
- bieżący monitoring newralgicznych punktów systemu bezpieczeństwa narażonych w szczególny sposób na ataki cybernetyczne, zwłaszcza dzięki wykorzystaniu zespołów CERT (*Computer Emergency Response Team*);
- prowadzenie audytu środków i mechanizmów cyberbezpieczeństwa z uwzględnieniem przyjętych standardów;
- przewidywanie i wdrażanie scenariuszy postępowania w np. sytuacjach cyberataków wymierzonych w cyfryzowane zadania państwa;

- rozwijanie i bieżąca aktualizacja – z punktu widzenia cyberbezpieczeństwa – planów reagowania kryzysowego oraz operacyjnych planów funkcjonowania w czasie zagrożenia i wojny, szczególnie pod kątem wpływu na systemy kierowania w państwie, z uwzględnieniem stosownych planów NATO i UE;
- prowadzenie aktywnej obrony i działań ofensywnych oraz utrzymanie gotowości do cyberwojny;
- ochrona i obrona własnych systemów i zgromadzonych w nich zasobów;
- wspieranie pozostałych kluczowych sektorów funkcjonujących w cyberprzestrzeni w zakresie zapewniania ich cyberbezpieczeństwa;
- przeciwdziałanie i zwalczanie cyberprzestępczości;
- bieżące działania informacyjne i edukacyjne skierowane do społeczeństwa w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz informowanie o zidentyfikowanych zagrożeniach.

30. Główne zadania w sektorze publicznym na poziomie międzynarodowym:
    - udział w międzynarodowym (przede wszystkim na forach NATO i Unii Europejskiej) reagowaniu na zagrożenia w cyberprzestrzeni;
    - międzynarodowa wymiana doświadczeń i dobrych praktyk w celu podnoszenia skuteczności działań krajowych;
    - oddziaływanie na transnarodowe struktury sektora prywatnego za pośrednictwem organizacji międzynarodowych;
    - wymiana informacji o podatnościach, zagrożeniach i incydentach.

31. Główne zadania w sektorze prywatnym:
    - współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom cybernetycznym, w tym opracowywanie własnych propozycji regulacji prawnych oraz samoregulacja sektora prywatnego wspierająca bezpieczeństwo w cyberprzestrzeni;
    - prowadzenie audytu środków i mechanizmów cyberbezpieczeństwa z uwzględnieniem standardów bezpieczeństwa ustanowionych dla sektora publicznego i promowanych wśród podmiotów sektora prywatnego narażonych w szczególny sposób na cyberataki;
    - współpraca z sektorem publicznym w zakresie wymiany informacji dotyczących istniejących oraz nowych zagrożeń dla cyberbezpieczeństwa.
    - wymiana informacji o podatnościach, zagrożeniach i incydentach.

32. Główne zadania w sektorze obywatelskim:
    - udział w narodowym wysiłku na rzecz bezpieczeństwa państwa poprzez należytą dbałość o użytkowane indywidualne systemy i urządzenia teleinformatyczne oraz samokształcenie obywateli w tym zakresie;
    - wykorzystanie mechanizmów zaangażowania obywatelskiego w celu monitorowania i ochrony prawa do prywatności i innych praw człowieka w internecie;
    - udział w społecznych inicjatywach obywatelskich wspierających cyberbezpieczeństwo RP (wolontariat dla cyberbezpieczeństwa, w tym także cyberobrony państwa).

33. Główne zadania transsektorowe:

- bieżąca koordynacja współpracy podmiotów sektora prywatnego i publicznego oraz stworzenie stosownych mechanizmów wymiany informacji (jawnych i niejawnych) oraz standardów i dobrych praktyk w obszarze cyberbezpieczeństwa (np. na drodze tworzenia przez instytucje państwowe programów certyfikacji bezpiecznego sprzętu i oprogramowania).
-

4. KONCEPCJA ZADAŃ PREPARACYJNYCH (PRZYGOTOWAWCZYCH) W DZIEDZINIE CYBERBEZPIECZEŃSTWA (UTRZYMANIA I ROZWOJU SYSTEMU CYBERBEZPIECZEŃSTWA RP)

34. Za najważniejsze zadania preparacyjne (przygotowawcze) w obszarze cyberbezpieczeństwa należy uznać wdrożenie i rozwijanie systemowego podejścia do cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym, które pozwoli na odpowiednią obronę i ochronę systemów teleinformatycznych przy zachowaniu ich efektywności i elastyczności realizacji procesów oraz zadań wykonywanych z wykorzystywaniem tych systemów.

35. Działania, których celem jest przyjęcie nowych rozwiązań prawnych, dotyczą zwłaszcza:

- stworzenia podstaw ciągłego funkcjonowania systemu teleinformatycznego, zapewniającego akceptowalny poziom bezpieczeństwa, szczególnie na potrzeby podsystemu kierowania bezpieczeństwem narodowym, w tym obronnością państwa;
- zapewnienia strukturalnego wsparcia i finansowania prac badawczo-rozwojowych w zakresie tworzenia nowych, narodowych rozwiązań w dziedzinie teleinformatyki i kryptologii;
- dokonania przeglądu i analizy istniejących w sferze cyberbezpieczeństwa regulacji w celu precyzyjnego określenia potrzeby ewentualnych zmian naprawczych i uzupełniających.

36. Istotne jest kształtowanie polskiego systemu cyberbezpieczeństwa w kontekście dokumentów UE i innych międzynarodowych inicjatyw w tym zakresie tak, aby był on wewnętrznie spójny oraz kompatybilny z podobnymi systemami państw sojuszniczych i organizacji międzynarodowych, których członkiem jest Polska (NATO, UE).

4.1 PODSYSTEM KIEROWANIA

37. Rada Ministrów jest odpowiedzialna za koordynację działań w zakresie cyberbezpieczeństwa na poziomie strategicznym. Wskazane jest ustanowienie lub poszerzenie zadań i kompetencji istniejącego ponadresortowego organu pomocniczego Rady Ministrów w sprawach szeroko rozumianego cyberbezpieczeństwa RP. Organ ten powinien mieć kompetencje doradcze, konsultacyjne i koordynacyjne, w tym dotyczące spraw przygotowywania – w ramach współpracy podmiotów sektora publicznego i prywatnego oraz przedstawicieli społeczeństwa obywatelskiego – odpowiednich rozwiązań i standardów, a także kompetencję koordynacji współpracy międzynarodowej w obszarze cyberbezpieczeństwa. Docelowo podmiot taki mógłby stać się częścią szerszego organu ponadresortowego ds. bezpieczeństwa narodowego[8].

38. Istotnym krokiem w kierunku zapewnienia pełnej efektywności systemu kierowania cyberbezpieczeństwem powinno być tworzenie technicznych centrów kompetencyjnych podporządkowanych właściwym ministrom. Ich zadaniem stałoby się zapewnienie akceptowalnego poziomu bezpieczeństwa usług teleinformatycznych, jako platformy

[8] W SPBN proponowany jest Rządowy Komitet Bezpieczeństwa Narodowego (z obsługującym go RCBN w ramach KPRM), którego częścią zadań byłyby sprawy cyberbezpieczeństwa.

dla działalności gospodarczej, e-administracji i funkcjonowania swobód obywatelskich oraz budowy zdolności obronnych w cyberprzestrzeni.

39. W ramach utrzymania i rozwoju podsystemu kierowania cyberbezpieczeństwem szczególnie istotne jest:
    - opracowywanie i wdrażanie zasad i procedur (z uwzględnieniem tzw. dobrych praktyk) kierowania cyberbezpieczeństwem, w tym zwłaszcza współpracy między sektorem publicznym a prywatnym;
    - ciągła modernizacja techniczna podsystemu kierowania, z uwzględnieniem wdrożenia bezpiecznych środków kierowania;
    - zbudowanie niezależnej sieci łączności kierowania bezpieczeństwem narodowym (np. w ramach sieci łączności rządowej) oraz zapewnienie narodowej kontroli systemów teleinformatycznych;
    - wypracowywanie minimalnych standardów cyberbezpieczeństwa dla infrastruktury krytycznej;
    - opracowywanie planów ćwiczeń i szkoleń w zakresie cyberbezpieczeństwa – ponadto, poza organizowaniem ćwiczeń wyłącznie w zakresie cyberbezpieczeństwa, problematyka ta powinna być uwzględniana w innych przedsięwzięciach szkoleniowych (na przykład ćwiczeniach w zakresie zarządzania kryzysowego i szkoleniach obronnych);
    - określenie wymogów i celów dla programów edukacyjnych, informacyjnych i oraz badawczych.

4.2. OGNIWA OPERACYJNE

40. Przygotowanie (utrzymanie i rozwój) operacyjnych ogniw systemu cyberbezpieczeństwa powinno mieć na celu zapewnienie adekwatnych środków i kompetencji do dynamicznie zmieniających się potrzeb operacyjnych. Z tego punktu widzenia szczególnie istotne jest:
    - stworzenie mechanizmów ochronnych i obronnych szybko adaptujących się do zmieniającego się środowiska bezpieczeństwa, zapewniających reagowanie na nieprzewidziane sytuacje kryzysowe;
    - uzyskanie zdolności do operatywnego zarządzania środkami cyberbezpieczeństwa;
    - zapewnienie bezpiecznego przepływu informacji między operacyjnymi ogniwami systemu cyberbezpieczeństwa;
    - budowanie zdolności prowadzenia aktywnych działań w cyberprzestrzeni.

41. Siły Zbrojne RP powinny dysponować zdolnościami obrony i ochrony własnych systemów i zgromadzonych w nich zasobów oraz aktywnej obrony i działań ofensywnych w cyberprzestrzeni zintegrowanymi z pozostałymi zdolnościami SZ RP, tak aby zwiększyć narodowy potencjał odstraszania (zniechęcania, powstrzymywania) potencjalnego agresora. W szczególności powinny być gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na większą skalę w razie cyberkonfliktu, w tym cyberwojny.

42. Konieczne jest tworzenie i wzmacnianie przeznaczonych do takich zadań jednostek. Istotne jest też rozwijanie narodowych zdolności w zakresie rozpoznawania, zapobiegania i zwalczania cyberzagrożeń.

43. Niezbędna jest implementacja standardów NATO dotyczących cyberobrony, zwłaszcza w kontekście planowania obronnego i operacyjnego. Konieczne jest również uwzględnianie

minimalnych standardów wypracowywanych przez NATO w zakresie ochrony zasobów własnych Sojuszu oraz zasobów krajowych infrastruktury krytycznej niezbędnej do realizacji zadań wynikających z członkostwa w Sojuszu.

44. Potrzebne jest rozwijanie zdolności służb wywiadowczych i kontrwywiadowczych do działania w cyberprzestrzeni, zapewniających skuteczną neutralizację aktywności obcych służb wywiadowczych i przeciwdziałanie szpiegostwu prowadzonemu z wykorzystywaniem nowych technologii.

45. Należy dążyć do nabycia pełnych kompetencji oraz zdolności do wytwarzania polskich rozwiązań technologicznych przeznaczonych do zapewnienia akceptowalnego poziomu bezpieczeństwa w cyberprzestrzeni. Znaczenie strategiczne ma zapewnienie uzyskiwania kontroli nad podsystemami informatycznymi uzbrojenia i innego sprzętu produkcji zagranicznej wykorzystywanego dla celów bezpieczeństwa narodowego. Szczególne istotne są zdolności w dziedzinie kryptologii, również w kontekście takiego rozwoju krajowego systemu cyberbezpieczeństwa, który pozwoli dostosowywać go do dynamicznie zmieniających się potrzeb.

46. Potrzebny jest rozwój w pełni kontrolowanych przez państwo narzędzi eleinformatycznych i technologii, przy zachowaniu zgodności z narzędziami oraz technologiami NATO i sojuszników, na których oparta byłaby obrona i ochrona krytycznych systemów państwa.

4.3. PUBLICZNE I PRYWATNE OGNIWA WSPARCIA

47. Należy zapewnić budowę narzędzi i mechanizmów oddziaływania podmiotów sektora prywatnego oraz społeczeństwa obywatelskiego na publiczne działania w zakresie cyberbezpieczeństwa, które pozwolą na osiągnięcie realnej synergii współdziałania publiczno-prywatnego na rzecz cyberbezpieczeństwa RP.

48. Istnieje również potrzeba zapewnienia odpowiednich mechanizmów współpracy oraz partnerstwa sektorów publicznego i prywatnego w dziedzinie cyberbezpieczeństwa. Ważnymi elementami działań wspólnej dbałości o cyberbezpieczeństwo państwa mogą stać się:

- dialog publiczno-prywatny w zakresie przygotowywania nowych rozwiązań legislacyjnych w celu tworzenia efektywnych rozwiązań, odpowiadających realnym wyzwaniom i zagrożeniom w środowisku bezpieczeństwa;
- tworzenie platformy porozumienia co do celów i zadań systemu cyberbezpieczeństwa poprzez dialog na poziomie teoretycznym oraz praktycznym;
- promowanie na poziomie krajowym oraz międzynarodowym narodowych rozwiązań i produktów w dziedzinie bezpieczeństwa;
- zapewnienie efektywnej współpracy i wsparcia państwowego w dziedzinie bezpieczeństwa, szczególnie dla prywatnych operatorów elementów infrastruktury krytycznej sterowanych przy użyciu systemów teleinformatycznych oraz operatorów i dostawców usług teleinformatycznych;
- uczestnictwo przedstawicieli sektora publicznego, prywatnego oraz obywateli w ciągłym procesie kształcenia i podwyższania świadomości o zagrożeniach w obszarze cyberbezpieczeństwa RP.

49. Istotne jest stworzenie systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa oraz szeroko rozumianej edukacji, w tym realizowanych we współpracy i partnerstwie zarówno ze światem nauki, jak i z przedsiębiorstwami komercyjnymi. Stworzenie podstaw takiej współpracy, uwzględniających tworzenie

systemu certyfikacji krajowych rozwiązań, będzie stanowiło ważny krok w dążeniu do narodowej niezależności w wymiarze technicznym, programistycznym i kryptologicznym.

50. Dla długoterminowej optymalizacji systemu cyberbezpieczeństwa RP należy stworzyć odpowiednie standardy branżowe i dobre praktyki wspierające organizacje prywatne oraz niepubliczne (NGO, instytucje naukowo-badawcze) w zarządzaniu ryzykiem w obszarze cyberbezpieczeństwa, także poprzez dostarczanie narzędzi do identyfikacji luk w ich systemach oraz opracowanie planu ich ciągłego doskonalenia.

51. Stworzone powinny być programy kształcenia przygotowujące kadry na potrzeby systemu cyberbezpieczeństwa (także stosowne ścieżki kariery pozwalające na przyciągnięcie najlepszych specjalistów).

52. Szczególnie ważne dla przygotowania efektywnego systemu cyberbezpieczeństwa będzie stworzenie systemowych podstaw dla wykorzystania potencjału obywateli RP (niebędących członkami SZ RP, ani innych służb czy instytucji państwowych) w drodze współpracy publiczno-prywatnej, co pozwoli na znaczne zwiększenie potencjału cyberbezpieczeństwa państwa.

53. Ważne jest prowadzenie działań informacyjnych i edukacyjnych o charakterze prewencyjnym i profilaktycznym w zakresie przygotowania obywateli do ich ochrony (w tym samoochrony) przed zagrożeniami w cyberprzestrzeni.

54. Potrzebne jest uznanie indywidualnego użytkownika, jego umiejętności i świadomości bezpieczeństwa, za jeden z filarów cyberbezpieczeństwa państwa oraz stosowne do tego kształtowanie mechanizmów przekazywania wiedzy oraz umiejętności co znacznie zwiększa prawdopodobieństwo osiągnięcia pożądanego poziomu bezpieczeństwa w cyberprzestrzeni.

ZAKOŃCZENIE

55. Doktryna cyberbezpieczeństwa RP powinna stanowić podstawę koncepcyjną podejmowania działań na rzecz cyberbezpieczeństwa RP. Wskazuje główne kierunki działań na poziomie strategicznym.

56. Treści Doktryny przewidziane są do uwzględniania i rozwijania w Polityczno-Strategicznej Dyrektywie Obronnej oraz w kolejnej edycji Strategii (Programu) Rozwoju Systemu Bezpieczeństwa Narodowego, a także w planach zarządzania kryzysowego oraz planach operacyjnych funkcjonowania struktur państwa w czasie zagrożenia i wojny.

57. Rekomendacje ujęte w niniejszej Doktrynie powinny być stosownie wykorzystywane przez wszystkie podmioty publiczne i prywatne odpowiedzialne za planowanie, organizowanie i realizowanie zadań w dziedzinie cyberbezpieczeństwa.

KONCEPCJA REFORMY NARODOWYCH SIŁ REZERWOWYCH

Reforma Narodowych Sił Rezerwowych była jednym z najważniejszych zadań wskazanych przez Prezydenta RP Bronisława Komorowskiego w marcu 2014 r., podczas odprawy kadry kierowniczej Ministerstwa Obrony Narodowej i Sił Zzbrojnych RP, dotyczących wzmocnienia strategicznej odporności kraju na agresję.

Przygotowane przez BBN założenia reformy były wynikiem prac prowadzonych m.in. w ramach Strategicznego Forum Bezpieczeństwa z udziałem przedstawicieli Ministerstwa Obrony Narodowej i Sił Zbrojnych RP, przedstawicieli proobronnych organizacji pozarządowych, a także ekspertów ds. bezpieczeństwa (w tym z Akademii Obrony Narodowej).

19 listopada 2014 r. koncepcja została przekazana do Ministerstwa Obrony Narodowej.

19 listopada 2014 r.

KONCEPCJA REFORMY NARODOWYCH SIŁ REZERWOWYCH

STRATEGICZNE ZADANIA NARODOWYCH SIŁ REZERWOWYCH:

a. Zadania operacyjne

- Lokalnie wspierać działania wojsk operacyjnych i innych służb państwa w zapewnianiu bezpieczeństwa terytorialnego;
- Uczestniczyć w działaniach nieregularnych na terytorium opanowanym przez przeciwnika.

b. Zadania preparacyjne (REFORMA)

- Odrębne formacje przy jednostkach wojskowych, przewidziane w operacyjne podporządkowanie WSzW („wojsko wojewodów");
- Oferta adresowana do rezerwistów – po zakończeniu służby zawodowej (służba post-zawodowa);
- Zróżnicowane (lokalnie) struktury i wyposażenie.

ZAŁOŻENIA OGÓLNE:

1. Analizując funkcjonujący dzisiaj model NSR – stanowiących *de facto* rozproszony zasób żołnierzy rezerwy obsadzających głównie wakaty, traktowanych przez dowódców jako „zło konieczne", faktycznie pełniących służbę zaledwie ułamek czasu w porównaniu z żołnierzami zawodowymi, dodatkowo – w formule ćwiczeń, a nie realnego użycia do konkretnych zadań – trudno nie zgodzić się z tezą, że jakość takiego uzupełnienia wojsk operacyjnych jest wątpliwa. O ile można było zrozumieć tolerowanie tego „oszczędnościowego" rozwiązania w ekspedycyjnym modelu armii, koncentrującym się na potrzebach zagranicznych operacji i poświęcającym mniejszą uwagę obronie terytorium kraju, w dzisiejszych realiach musi ono budzić poważną refleksję: stwarza bowiem mylne wrażenie posiadania adekwatnych liczebnie, odpowiednio wyszkolonych i przygotowanych, aktywnych rezerw sił zbrojnych – odsuwając w czasie prawdziwe rozwiązanie tego problemu. Jest również niezgodne z „doktryną Komorowskiego" – powrotu do priorytetowego traktowania obrony terytorium państwa.Dodatkowo, kontynuowanie stanu rzeczy, w którym swoiste „martwe dusze", jakimi w znacznym stopniu pozostają żołnierze NSR – są wliczane do stanu sił zbrojnych i uwzględniane przy kwalifikowaniu jednostek do poszczególnych kategorii gotowości bojowej – jest nie do przyjęcia w dzisiejszych uwarunkowaniach bezpieczeństwa. Tak definiowana gotowość bojowa jest w dużym stopniu pozorna. Ubocznym skutkiem tworzenia NSR w ramach etatu SZ RP, przy jednoczesnym rozbudowaniu biurokratycznych regulacji dotyczących kwestii etatowych w wojsku, jest

usztywnienie struktury sił zbrojnych. Każda zmiana organizacyjna w jednym miejscu, wymaga cięć i przesunięć etatowych w innym, mimo istniejących fizycznie wakatów. Ta sprawa również wymaga nowego, systemowego rozwiązania, zwłaszcza w kontekście dużych programów modernizacyjnych, które przecież implikują modyfikację istniejących oraz tworzenie nowych struktur organizacyjnych w wojsku. BBN ma w tym obszarze konkretne rekomendacje.

2. Reforma NSR powinna być częścią reformy całego systemu rezerw Sił Zbrojnych RP. Tylko wówczas zapewnimy utrzymywanie zdolności armii do prowadzenia długotrwałych operacji w czasie P/K/W (przy okazji, „*sustainability*" – to także jedno z sojuszniczych kryteriów przyjętych przez Polskę, na równi z deklaracją przeznaczania 2 proc. PKB na obronność). Kwalifikowane rezerwy osobowe wojska wyczerpują się. Negatywną tendencję kurczenia się zasobów wyszkolonych rezerw powstrzymało dopiero Rozporządzenie Rady Ministrów z dnia 20 lutego 2013 r., *w sprawie obowiązkowych ćwiczeń wojskowych dla żołnierzy rezerwy*, które potwierdziło dostrzeżenie tego problemu przez resort obrony. Należy jednak zwrócić uwagę, że to rozwiązanie – odnosząc się wyłącznie do żołnierzy będących już w rezerwie – nie zapewnia uzupełniania rezerw o nowe zasoby. W dzisiejszym stanie prawnym nowe rezerwy mobilizacyjne mogą tworzyć żołnierze kończący służbę zawodową (zaledwie kilka tysięcy rocznie) oraz... żołnierze NSR (osoby rezygnujące ze służby w NSR otrzymują przydziały mobilizacyjne) – chociaż nie taki był cel utworzenia tych sił.

3. Zmiany proponowane przez BBN zmierzają – w uproszczeniu – do powrotu do pierwotnej koncepcji NSR przedstawionej w „Programie profesjonalizacji SZ RP". Uczynienie z NSR przedsionka służby zawodowej odwróciło ideę formacji „post-zawodowej" na „przed-zawodową", zmieniając adresata oferty tej służby. Stworzono tym samym fałszywą motywację wstępowania do NSR, sztucznie zwiększając zainteresowania tą formą służby, przy okazji narażając na szwank rozpoznawalny „znak firmowy". Prawdziwym celem większości żołnierzy dzisiejszych NSR jest służba zawodowa. Efektem ubocznym było zrównanie szkolenia (a tym samym wymagań) do służby zawodowej i niezawodowej; w praktyce „wygaszono" służbę kandydacką do służby zawodowej (z wyjątkiem małej grupy oficerów). Można zaryzykować stwierdzenie, że w odniesieniu do służby zawodowej – NSR stanowią zbędny etap pośredni.

4. Jak wynika z audytów przeprowadzonych niedawno w Stanach Zjednoczonych oraz Wielkiej Brytanii, oszczędności będące konsekwencją szerokiego wykorzystywania sił rezerwowych, a które legły u podstaw polskich rozwiązań – mają charakter względny. 20-procentowy koszt sił rezerwowych w porównaniu z siłami regularnymi można odnosić tylko do okresu szkolenia. Podczas realnego wykorzystania tych sił koszty rosną do 87 proc. kosztów generowanych przez formacje służby stałej i to przy założeniu, że pozostałe wydatki związane z użyciem rezerw (przerzut sił, etc.) – pokrywa skarb państwa. Reasumując – siły rezerwowe są tańsze tylko wtedy, kiedy się szkolą i fakt ten należy uwzględniać w projektowaniu budżetu sił zbrojnych.

5. Problem NSR nakłada się na kwestię obligatoryjnych zwolnień ponad 40 tys. szeregowych w ciągu najbliższych 10 lat – z uwagi na upłynięcie 12 lat ich służby. Dzisiaj NSR „blokują" ok. 5,5 tys. etatów podoficerskich, które mogłyby być rozwiązaniem dla grupy najlepszych szeregowych z doświadczeniem bojowym i umożliwić im pozostanie w służbie po spełnieniu warunków przejścia do korpusu podoficerów. To problem zasługujący na szczególną uwagę.

6. Koncepcja BBN ma w zamyśle odwrócić negatywny trend i przywrócić Narodowym Siłom Rezerwowym charakter służby post-zawodowej, pełnionej przez byłych żołnierzy w lokalnych, jednolitych formacjach rezerwowych. Obsadzenie pojedynczego etatu w regularnej jednostce przez żołnierza NSR powinno być wyjątkiem, a nie regułą. BBN proponuje rozważenie wtórnego „uzawodowienia" ok. 10 tys. etatów zajmowanych przez żołnierzy NSR – w drodze powołania najlepszych żołnierzy (ochotniczo) do służby zawodowej. Spowodowałoby to – po okresie niezbędnego doszkolenia – znaczące

podniesienie potencjału sił zbrojnych i urealnienie kategorii gotowości bojowej jednostek w ramach limitu 120 tys. etatów w siłach zbrojnych.

7. Rozwiązania wymaga kwestia ewentualnych, nowych form służby przed-zawodowej, o ile utrzyma się na nią dotychczasowe, stosunkowo wysokie społeczne zapotrzebowanie. Należy rozważyć wykorzystanie w tym celu potencjału organizacji proobronnych, a także stworzenie możliwości certyfikowanego szkolenia wojskowego dla zainteresowanych osób, bez konieczności podejmowania służby wojskowej. Potrzebne są również regulacje prawne umożliwiające rozszerzenie szkolenia nowych rezerw mobilizacyjnych.

PODSUMOWANIE:

Zarysowanie powyżej dylematy pokazują, jak złożonym i wielowymiarowym problemem jest sanacja systemu rezerw sił zbrojnych. O ile prace nad szczegółami koncepcji reformy powinny zostać uruchomione możliwie pilnie, proces ich wdrażania powinien zostać rozłożony w czasie i poprzedzony analizą korzyści oraz oceną ryzyk tak, aby nie zaprzepaścić osiągnięć programu profesjonalizacji, ale jednocześnie zwiększyć zarówno jakość zasobów rezerwowych sił zbrojnych (ich wartość operacyjną) oraz ich liczebność – w możliwie rozsądnym czasie. Niezwykle ważna będzie strategia komunikacji społecznej – informowania o inicjatywach podejmowanych w tym obszarze, w celu budowania społecznego zrozumienia i poparcia.

REKOMENDACJE SZCZEGÓŁOWE:

1. Problem zmiany nazwy NSR na Armię Krajową, Gwardię Narodową, itp. Istnieją formalno-prawne ograniczenia dotyczące używania nazw historycznych. Dlatego należy albo pozostawić dotychczasową nazwę, albo poszukiwać innej, zgodnej z istotą tych wojsk, np. Terenowe/Terytorialne Wojska Rezerwy Operacyjnej.
2. Wojewódzkie/terenowe oddziały NSR, istniejące zalążkowo na stałe na bazie organizacyjno-infrastrukturalnej wojska w każdym województwie. Podległe pod Wojewódzkie Sztaby Wojskowe (WSzW).
3. W czasie „P" prowadzą cykliczne szkolenie i utrzymują gotowość do szybkiego rozwinięcia kryzysowego lub mobilizacyjnego na czas zagrożenia lub wojny. Współpracują z organizacjami proobronnymi.
4. Zadania NSR – komplementarne z zadaniami operacyjnymi wojewody w zakresie bezpieczeństwa na czas P/K/W.
5. Struktura dostosowana do lokalnych potrzeb, wynikających z operacyjnych planów funkcjonowania województwa w czasie zagrożenia i wojny, jednolita na czas P/K/W.
6. Liczebność: należy poszukiwać rozwiązania na poziomie określonym w programie profesjonalizacji, czyli do 120 tys. żołnierzy służby czynnej i NSR. Rekomenduje się wykorzystanie reformy do zwiększenia liczby żołnierzy zawodowych do 110 tys. oraz ustanowienia liczby NSR czasu pokojowego na poziomie 10 tys. żołnierzy rezerwy.
7. Należy przywrócić zawodowy charakter stanowisk zajmowanych obecnie w jednostkach wojskowych przez żołnierzy NSR i obsadzić je (w pierwszej kolejności) chętnymi żołnierzami NSR, powołując ich do służby zawodowej – zgodnie z deklarowanymi oczekiwaniami większości z nich. Praktykowane obecnie obsadzanie etatów jednostek wojskowych niezawodowymi żołnierzami NSR jest patologią (niezawodowy żołnierz rezerwy na etacie żołnierza zawodowego) – podlegającą ciągłej (i zasłużonej) krytyce.

8. Proces uzupełnienia „uwolnionych” etatów żołnierzami zawodowymi należy prowadzić planowo, etapami (kwestia zaszeregowania jednostek do odpowiednich kategorii gotowości).
9. Finansowanie. Zgodnie z programem profesjonalizacji SZ RP obejmują 120 tys. etatów żołnierzy zawodowych – i na taką liczbę żołnierzy powinny być zabezpieczone środki finansowe. Innymi słowy – nieformalne ograniczenia finansowe („limity” uzgadniane z ministerstwem finansów) – nie mogą być argumentem przeciwko proponowanemu rozwiązaniu w sytuacji, gdy istnieje polityczna zgoda co do liczebności sił zbrojnych na poziomie 120 tys.

STRATEGIA BEZPIECZEŃSTWA NARODOWEGO RZECZYPOSPOLITEJ POLSKIEJ

Strategia Bezpieczeństwa Narodowego RP, będąca najważniejszym dokumentem w państwie dotyczącym bezpieczeństwa narodowego, zatwierdzona została przez Prezydenta RP Bronisława Komorowskiego, na wniosek Prezesa Rady Ministrów, 5 listopada 2014 r.

Dokument przygotowany został przy ścisłej współpracy z Biurem Bezpieczeństwa Narodowego przez międzyresortowy zespół do spraw opracowania Strategii.

5 listopada 2014 r.

STRATEGIA BEZPIECZEŃSTWA NARODOWEGO RZECZYPOSPOLITEJ POLSKIEJ

WSTĘP

1. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* jest dokumentem dotyczącym bezpieczeństwa państwa, opracowywanym i zatwierdzanym zgodnie z art. 6 ust. 1 i art. 4a ust. 1 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2012 r. poz. 461, z późn. zm.). Strategia w sposób całościowy ujmuje zagadnienia bezpieczeństwa narodowego oraz wskazuje optymalne sposoby wykorzystania na potrzeby bezpieczeństwa wszystkich zasobów pozostających w dyspozycji państwa w sferze obronnej, ochronnej, społecznej i gospodarczej. Kluczową sprawą jest ich właściwa integracja w systemie bezpieczeństwa narodowego.

2. Prezentowany dokument identyfikuje interesy narodowe i cele strategiczne w dziedzinie bezpieczeństwa, w zgodzie z zasadami i wartościami zawartymi w *Konstytucji Rzeczypospolitej Polskiej*. Określa potencjał bezpieczeństwa narodowego oraz ocenia środowisko bezpieczeństwa Polski w wymiarze globalnym, regionalnym i krajowym, a także prognozuje jego trendy rozwojowe. Przedstawia działania państwa niezbędne dla osiągnięcia zdefiniowanych interesów i celów oraz wskazuje kierunki i sposoby przygotowania systemu bezpieczeństwa narodowego.

3. Zapisy dokumentu są zbieżne ze strategiami Organizacji Traktatu Północnoatlantyckiego (NATO) i Unii Europejskiej (UE) oraz dokumentami strategicznymi tworzącymi nowy system zarządzania rozwojem kraju, w szczególności ze średniookresową strategią rozwoju kraju oraz koncepcją przestrzennego zagospodarowania kraju. W przygotowaniu *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* wykorzystano wyniki Strategicznego Przeglądu Bezpieczeństwa Narodowego zakończonego w 2012 r. – pierwszego tak szeroko zakrojonego projektu analitycznego odnoszącego się do stanu systemu bezpieczeństwa narodowego i kierunków jego rozwoju.

ROZDZIAŁ I. POLSKA JAKO PODMIOT BEZPIECZEŃSTWA

4. Rzeczpospolita Polska jest samodzielnym podmiotem bezpieczeństwa, suwerennie określającym własne interesy narodowe i cele strategiczne. Wynikają one z doświadczeń historycznych, istniejących warunków polityczno-ustrojowych oraz potencjału, jakim dysponuje państwo.

1.1. Polska w Europie i świecie

5. Polska jest demokratycznym państwem prawnym z gospodarką rynkową, przestrzegającym wiążącego ją prawa międzynarodowego. Polska wzmacnia swój potencjał bezpieczeństwa narodowego, aby zapewnić stabilny rozwój kraju oraz poprawę warunków życia obywateli. Jest aktywnym uczestnikiem współpracy międzynarodowej i rozwija przyjazne stosunki oraz współpracę z państwami bliższego i dalszego sąsiedztwa.

6. Członkostwo w euroatlantyckich i europejskich strukturach współpracy wzmacnia bezpieczeństwo Rzeczypospolitej Polskiej. NATO stanowi najważniejszą formę polityczno-wojskowej współpracy Polski z sojusznikami. Unia Europejska wspiera rozwój społeczno-gospodarczy Polski i umacnia jej pozycję w świecie. Najważniejszym partnerem pozaeuropejskim Polski pozostają Stany Zjednoczone Ameryki.

7. W międzynarodowej polityce bezpieczeństwa systematycznie rośnie znaczenie współpracy regionalnej. Dla Polski kluczowymi ugrupowaniami w tym zakresie są Trójkąt Weimarski i Grupa Wyszehradzka. W ich ramach dobrze rozwijają się także dwustronne relacje polityczno-wojskowe z tworzącymi je państwami. Poszukiwane są nowe płaszczyzny współdziałania między innymi z Litwą, Łotwą, Estonią i Grupą Nordycką oraz Rumunią, a także w innych regionach Europy.

8. Rzeczpospolita Polska wspiera reformy państw Partnerstwa Wschodniego oraz opowiada się za ich ściślejszym powiązaniem z UE i NATO. Punktem wyjścia tych działań są zasady wolności, demokracji, gospodarki rynkowej oraz otwartej perspektywy integracyjnej

z euroatlantyckimi instytucjami je wyrażającymi. Jako sąsiad Federacji Rosyjskiej Polska stoi na stanowisku, że zarówno stosunki dwustronne, jak i stosunki NATO-Rosja i UE-Rosja powinny rozwijać się w oparciu o pełne poszanowanie prawa międzynarodowego, w tym suwerenności i integralności terytorialnej państw, a także swobody wyboru własnej ścieżki rozwoju i sojuszy politycznych i wojskowych.

9. Polska jest wiarygodnym członkiem Organizacji Narodów Zjednoczonych (ONZ), odpowiedzialnej za utrzymanie pokoju i bezpieczeństwa międzynarodowego oraz Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), istotnego elementu europejskiego systemu kooperatywnego bezpieczeństwa.

10. Na miarę swoich możliwości oraz interesów, jako część wspólnoty międzynarodowej, Polska angażuje się w rozwiązywanie problemów globalnych. Utrzymuje stosunki dyplomatyczne z pozaeuropejskimi partnerami oraz rozwija z nimi obustronnie korzystną współpracę polityczną i gospodarczą.

1.2. Interesy narodowe i cele strategiczne

11. Rzeczpospolita Polska zapewnia bezpieczeństwo państwa i obywateli poprzez stwarzanie warunków do realizacji interesów narodowych i osiągania celów strategicznych. Interesy narodowe określa art. 5 Konstytucji Rzeczypospolitej Polskiej. Z nich wynikają **interesy narodowe w dziedzinie bezpieczeństwa**, do których należą:

- dysponowanie skutecznym narodowym potencjałem bezpieczeństwa zapewniającym gotowość i zdolność do zapobiegania zagrożeniom, w tym odstraszania, obrony i ochrony przed nimi oraz likwidowania ich następstw;
- silna pozycja międzynarodowa Polski i członkostwo w wiarygodnych systemach bezpieczeństwa międzynarodowego;
- ochrona indywidualna i zbiorowa obywateli przed zagrożeniami dla ich życia i zdrowia oraz przed naruszeniem, utratą lub degradacją istotnych dla nich dóbr (materialnych i niematerialnych);
- zapewnienie swobody korzystania przez obywateli z wolności i praw, bez szkody dla bezpieczeństwa innych osób i bezpieczeństwa państwa oraz zapewnienie tożsamości narodowej i dziedzictwa kulturowego;
- zapewnienie trwałego i zrównoważonego rozwoju potencjału społecznego i gospodarczego państwa, ze szczególnym uwzględnieniem ochrony środowiska naturalnego oraz warunków życia i zdrowia ludności jako podstawy bytowania.

12. Z powyższego układu interesów wynikają odpowiadające im **cele strategiczne w dziedzinie bezpieczeństwa**:

- utrzymywanie i demonstrowanie gotowości zintegrowanego systemu bezpieczeństwa narodowego do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania zagrożeniom;
- doskonalenie zintegrowanego systemu bezpieczeństwa narodowego, a zwłaszcza jego elementów kierowania, w tym zapewnienie niezbędnych zasobów i zdolności;
- rozwój potencjału obronnego i ochronnego adekwatnego do potrzeb i możliwości państwa oraz zwiększenie jego interoperacyjności w ramach NATO i UE;
- wzmocnienie gotowości i zdolności NATO do kolektywnej obrony oraz spójności działań UE w dziedzinie bezpieczeństwa; budowanie silnej pozycji Polski w obu tych organizacjach;

- rozwijanie bliskiej współpracy ze wszystkimi sąsiadami oraz budowanie partnerskich relacji z innymi państwami, w tym służących zapobieganiu i rozwiązywaniu konfliktów i kryzysów międzynarodowych;
- promowanie na arenie międzynarodowej zasad prawa międzynarodowego oraz uniwersalnych wartości, takich jak: demokracja, prawa człowieka i wolności obywatelskie, a także podnoszenie w polskim społeczeństwie świadomości praw człowieka i obywatela;
- zapewnienie bezpieczeństwa powszechnego poprzez doskonalenie krajowego systemu ratowniczo-gaśniczego oraz systemu monitorowania, powiadamiania, ostrzegania o zagrożeniach i likwidowania skutków klęsk żywiołowych oraz katastrof, a także wdrożenie rozwiązań prawnych i organizacyjnych w zakresie systemu ochrony ludności oraz obrony cywilnej;
- doskonalenie i rozwój krajowego systemu zarządzania kryzysowego w kierunku zapewnienia jego wewnętrznej spójności i integralności oraz umożliwienia niezakłóconej współpracy w ramach systemów zarządzania kryzysowego organizacji międzynarodowych, których Polska jest członkiem;
- ochrona granic Polski, stanowiących zewnętrzną granicę UE; przeciwdziałanie przestępczości zorganizowanej, w tym gospodarczej; ochrona porządku publicznego;
- udoskonalenie rozwiązań systemowych dla przeciwdziałania i zwalczania terroryzmu i proliferacji broni masowego rażenia;
- zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni;
- zapewnienie bezpiecznych warunków rozwoju kapitału ludzkiego i społecznego oraz innowacyjności, efektywności i konkurencyjności gospodarki, a także stabilności finansowej państwa;
- zapewnienie bezpieczeństwa energetycznego i bezpieczeństwa klimatycznego oraz ochrony środowiska, różnorodności biologicznej i zasobów naturalnych, w szczególności zasobów wodnych, a także kształtowanie zagospodarowania przestrzennego kraju w sposób zwiększający odporność na różnorakie zagrożenia, w szczególności militarne, naturalne i technologiczne;
- zapewnienie bezpieczeństwa żywnościowego;
- prowadzenie efektywnej polityki rodzinnej oraz dostosowanie polityki migracyjnej do nowych wyzwań;
- pogłębianie świadomości społecznej w sferze bezpieczeństwa oraz zwiększanie kompetencji obywateli pozwalających na właściwe reagowanie w sytuacjach kryzysowych.

13. Interesy narodowe i cele strategiczne w dziedzinie bezpieczeństwa przekładane są na strategiczne działania i zadania, stosownie do warunków bezpieczeństwa oraz możliwości ich wykonania.

1.3. Strategiczny potencjał bezpieczeństwa narodowego

14. Potencjał bezpieczeństwa narodowego służy realizacji interesów narodowych i osiąganiu celów strategicznych. Jego wzmacnianie wyraża dbałość o bezpieczeństwo Polski i jest wkładem w umacnianie zdolności obronnych NATO i UE.

15. **System bezpieczeństwa narodowego** obejmuje siły, środki i zasoby przeznaczone przez państwo do realizacji zadań w tym obszarze, odpowiednio zorganizowane, utrzymywane i przygotowywane. Składa się on z podsystemu kierowania i podsystemów wykonawczych, w

tym podsystemów operacyjnych (obronny i ochronne) oraz podsystemów wsparcia (społeczne i gospodarcze).

16. **Podsystem kierowania** jest kluczowym elementem systemu bezpieczeństwa narodowego. Tworzą go organy władzy publicznej i kierownicy jednostek organizacyjnych, wykonujący zadania związane z bezpieczeństwem narodowym, wraz z organami doradczymi i aparatem administracyjnym oraz procedurami funkcjonowania i stosowną infrastrukturą. Jego fundamentem są trwałe zasady ustrojowe. Szczególna rola w kierowaniu bezpieczeństwem narodowym przypada Parlamentowi, Prezydentowi Rzeczypospolitej Polskiej i Radzie Ministrów. Istotnym elementem podsystemu kierowania bezpieczeństwem narodowym jest zarządzanie kryzysowe.

17. **Podsystemy wykonawcze** to siły i środki przewidziane do realizacji zadań w obszarze bezpieczeństwa narodowego, pozostające w dyspozycji organów kierowania bezpieczeństwem. Dzielą się one na podsystemy: operacyjne (obronny i ochronne) oraz wsparcia (społeczne i gospodarcze). Podsystemy operacyjne przeznaczone są do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania zagrożeniom o charakterze polityczno-militarnym i pozamilitarnym. Podsystemy społeczne i gospodarcze zasilają je odpowiednimi zdolnościami i zasobami.

18. Konieczność rozwoju **potencjału obronnego** jest powszechnie akceptowana. Główny element potencjału obronnego stanowią profesjonalne Siły Zbrojne RP. Ich bezprecedensowa w swojej skali modernizacja techniczna, którą zabezpiecza ustawowo zagwarantowane, stabilne i długoterminowe finansowanie potrzeb obronnych państwa, prowadzi do pozyskania nowoczesnego sprzętu wojskowego oraz poszerzenia zdolności operacyjnych. Procesy modernizacyjne obejmują również różne aspekty funkcjonowania polskiej dyplomacji, służb specjalnych działających na rzecz obronności oraz polskiego przemysłu obronnego i związanego z nim potencjału naukowo-badawczego. Konsekwentnie realizowana polityka bezpieczeństwa, stanowiąca integralną część polskiej polityki zagranicznej, sprzyja wzmacnianiu potencjału obronnego w wymiarze militarnym i niemilitarnym.

19. Zróżnicowany wewnętrznie **potencjał ochronny** wspiera państwo w realizacji zadań z zakresu bezpieczeństwa narodowego. Tworzony jest on przez: wymiar sprawiedliwości; służby specjalne; państwowe służby, straże i inspekcje wyspecjalizowane w ochronie porządku publicznego, służby ratownictwa i ochrony ludności; elementy zarządzania kryzysowego; Straż Graniczną; Służbę Celną; podmioty sektora prywatnego (firmy ochrony osób i mienia); organizacje pozarządowe (zwłaszcza społeczne organizacje ratownicze). Istotną rolę odgrywają tu podmioty odpowiedzialne za ochronę bezpieczeństwa cybernetycznego oraz za przeciwdziałanie i zwalczanie terroryzmu i ekstremizmu.

20. **Potencjał społeczny**, w tym kapitał ludzki, jest ważnym czynnikiem warunkującym wzrost gospodarki narodowej, sprawność państwa, aktywność społeczeństwa obywatelskiego oraz ogólną poprawę jakości życia obywateli. Nowoczesny system edukacji publicznej i szkolnictwa wyższego, a także upowszechnienie różnych form uczenia się przez całe życie służą wykształceniu społeczeństwa aktywnego i mobilnego. Istotnym elementem rozwoju kapitału ludzkiego i społecznego jest edukacja na rzecz bezpieczeństwa.

21. **Potencjał gospodarczy.** W ostatnich dwóch dekadach gospodarka Polski rozwijała się w sposób ciągły. Stały wzrost Produktu Krajowego Brutto przekłada się na poprawę warunków życia społeczeństwa i zbliżanie wskaźników gospodarki narodowej do poziomu średniego PKB w Unii Europejskiej. Aktywność inwestycyjna polskich firm za granicą oraz rosnący eksport świadczą o rozwoju i coraz większej konkurencyjności polskiej gospodarki.

22. **Energetyka** jest jednym z kluczowych elementów bezpieczeństwa narodowego. Do głównych czynników bezpieczeństwa energetycznego należy dostęp do surowców energetycznych, w tym poza granicami kraju, dywersyfikacja źródeł i kierunków dostaw paliw oraz budowa nowych mocy w oparciu o zróżnicowane technologie wytwarzania, pozwalająca na zrównoważenie krajowego popytu na energię. Polityka energetyczna Polski ukierunkowana jest

na zapewnienie właściwego rozwoju infrastruktury wytwórczej, przesyłowej i magazynowej oraz stymulowanie inwestycji w nowoczesne, energooszczędne technologie i produkty, a także ograniczenia zależności od dostaw surowców energetycznych.

23. **System transportowy.** Nowoczesna sieć drogowa i kolejowa, rozwinięta sieć śródlądowych dróg wodnych, lotnisk, portów morskich oraz infrastruktura dostępu do tych portów, a także sprawny system transportu publicznego umożliwiają rozwój polskiej gospodarki i wzmacniają jej powiązanie z gospodarką światową. Są także ważnym składnikiem bezpieczeństwa narodowego oraz terytorialnie zrównoważonego rozwoju kraju. Nowoczesna infrastruktura transportowa, unowocześniony park taborowy oraz integralne systemy zarządzania przewozami obniżają koszty w gospodarce, przyczyniając się jednocześnie do obniżenia presji na środowisko. Systematyczna poprawa infrastruktury transportowej będzie stanowiła jedno z podstawowych wyzwań dla rozwoju państwa.

ROZDZIAŁ II. ŚRODOWISKO BEZPIECZEŃSTWA POLSKI

24. Współczesne środowisko bezpieczeństwa charakteryzuje zacieranie się granic między jego wymiarem wewnętrznym i zewnętrznym, militarnym i pozamilitarnym. Globalizacja i rosnąca współzależność często skutkują nieprzewidywalnością zjawisk, których zasięg nie jest już ograniczony barierami geograficznymi, systemami politycznymi i gospodarczymi. Nadal obecne są wyzwania i zagrożenia typu militarnego. Bezpieczeństwo Polski będzie zależało od jej zdolności do efektywnej realizacji interesów narodowych i osiągania celów strategicznych w obecnych i prognozowanych warunkach bezpieczeństwa. Dotyczy to w szczególności wykorzystania szans i sprostania wyzwaniom o charakterze wewnętrznym i zewnętrznym, asymetrycznym i transsektorowym, które są konsekwencją wzajemnie na siebie oddziałujących procesów i zjawisk politycznych, militarnych, ekonomiczno-społecznych, demograficznych i środowiskowych.

2.1. Wymiar globalny

25. Procesy globalizacji, tworzenie się wielobiegunowego porządku politycznego, zagrożenia militarne oraz szereg wyzwań o charakterze asymetrycznym wpływają na bezpieczeństwo i stabilność państw. W połączeniu z dysproporcjami rozwojowymi oraz rywalizacją międzypaństwową wzmagają one ryzyko wystąpienia konfliktów, sporów i napięć. Nie zniknęła groźba konfliktów o charakterze regionalnym i lokalnym.

26. **Organizacja Narodów Zjednoczonych** – jedyna struktura powołana w celu zapewnienia bezpieczeństwa globalnego, ma szczególną pozycję w systemie organizacji międzynarodowych. Niekorzystnym zjawiskiem są występujące w jej ramach obszary dysfunkcjonalności, niedecyzyjności oraz rywalizacji państw i grup regionalnych, co skutkuje obniżeniem legitymizacji i efektywności jej działań. Podstawowe znaczenie będzie miało podniesienie skuteczności i wiarygodności ONZ jako źródła legitymizowanych prawnie działań społeczności międzynarodowej w różnych sferach bezpieczeństwa globalnego.

27. Problemem globalnym pozostaną skutki działań państw pozostających poza systemem współpracy międzynarodowej, niestosujących się (lub czyniących to selektywnie) do norm prawa międzynarodowego. Podważanie powszechnie legitymizowanych norm pokojowego współistnienia państw prowadzi do osłabienia współczesnego porządku międzynarodowego.

28. Niepokój budzi postępujące w ostatnich latach **podważanie wiarygodności porozumień rozbrojeniowych**, w tym dotyczących nieproliferacji broni masowego rażenia. Wiąże się to z groźbą jej niekontrolowanego rozwoju, powstania nowego wyścigu zbrojeń czy uzyskania dostępu do tego typu broni przez ugrupowania terrorystyczne.

29. Problemem bezpieczeństwa światowego pozostanie utrzymywanie się **porządków autorytarnych** i postaw konfrontacyjnych, nieposzanowanie zasad prawa międzynarodowego, standardów demokratycznych, praw człowieka, mniejszości etnicznych i religijnych.

W przypadkach niektórych państw autorytarnych wiąże się to ze stworzeniem atrakcyjnych modeli gospodarczych, które rzucają wyzwanie systemom zachodniej demokracji i gospodarki rynkowej. Zwiększa to odpowiedzialność społeczności międzynarodowej za wspieranie i upowszechnianie demokracji, praworządności i bezpieczeństwa. Polska transformacja ustrojowa jest niezmiennie przykładem i źródłem dobrych praktyk dla państw przekształcających swoje systemy polityczne, prawne i gospodarcze.

30. Zagrożeniami dla globalnego bezpieczeństwa pozostaną **międzynarodowy terroryzm i zorganizowana przestępczość** jako składniki niestabilności i konfliktów wewnętrznych oraz źródła takich patologii, jak: przemyt broni, materiałów jądrowych i podwójnego zastosowania, handel narkotykami i ludźmi, porwania dla okupu oraz nielegalne operacje finansowe. Wyzwanie stanowią też niekontrolowane migracje ludności, wywołane zarówno przez konflikty, jak i mające swe źródło w problemach natury gospodarczej i społecznej.

31. Wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak **cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty** z udziałem podmiotów niepaństwowych i **cyberwojna**, rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. Przy rosnącym uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw.

32. Istotnym wyzwaniem dla bezpieczeństwa międzynarodowego stają się różne formy **ekstremizmu** o podłożu politycznym, religijnym, etnicznym, społeczno-ekonomicznym i innym. Są one szczególnie niebezpieczne, gdy wykorzystują terroryzm jako instrument działania. Zjawisko ekstremizmu może mieć zorganizowany charakter, jak również wynikać z działań pojedynczych osób.

33. W konsekwencji dynamicznego rozwoju społecznego, gospodarczego i technologicznego świata wyzwaniem staje się **wzrost zapotrzebowania na energię, żywność i wodę pitną**. Surowce energetyczne i metale ziem rzadkich występują często na obszarach niestabilnych politycznie, lub stają się narzędziami realizacji celów politycznych państw eksporterów. Rosnący popyt na żywność jest konsekwencją obserwowanej w wielu częściach świata eksplozji demograficznej, zmian klimatu oraz nierównomiernego rozwoju gospodarczego. Prowadzi to do wzrostu cen żywności i niezdolności niektórych państw do zaspokojenia potrzeb żywnościowych ludności. Kurczące się zasoby wody pitnej oraz znaczne zanieczyszczenie jej ujęć mogą w przyszłości stać się przyczyną konfliktów i wojen.

2.2. Wymiar regionalny

34. Bezpieczeństwo Europy determinowane będzie przez cztery główne czynniki: NATO, Unię Europejską, strategiczną obecność USA na kontynencie europejskim oraz relacje z Rosją. Istotne jest, by ewolucja bezpieczeństwa w Europie sprzyjała spójności i solidarności oraz rozwojowi zdolności obronnych NATO i UE, a nie obniżeniu poziomu ambicji państw członkowskich w tej mierze. Utrzymanie adekwatnego poziomu zdolności obronnych oraz wola polityczna do realizacji zobowiązań z dziedziny bezpieczeństwa będą zapobiegały organizacji procesów bezpieczeństwa według kryteriów różnych prędkości.

35. W przewidywalnej przyszłości Europa pozostanie kontynentem o zróżnicowanych zagrożeniach w wymiarze militarnym – większość państw prowadzi pogłębioną współpracę polityczno-wojskową i należy do struktur współpracy wielostronnej (NATO i UE). Mimo to nie brak dziś w Europie źródeł **potencjalnej destabilizacji**, wynikających ze sporów politycznych i terytorialnych, napięć etnicznych i religijnych, mogących przybrać charakter konfliktów zbrojnych. Jedynie trwałe rozwiązania pokojowe i stałe wsparcie wspólnoty międzynarodowej dają szansę na rozwiązanie konfliktów i eliminację ryzyka otwartej konfrontacji.

36. W sąsiedztwie Polski istnieje ryzyko konfliktów o charakterze regionalnym i lokalnym, mogących angażować ją pośrednio lub bezpośrednio. Polska nie jest też wolna od form nacisku politycznego wykorzystującego argumentację wojskową. W jej najbliższym otoczeniu występuje duże skupienie potencjałów wojskowych, także o konfiguracji ofensywnej. Zagrożenia dla Polski mogą w niesprzyjających okolicznościach przyjąć charakter niemilitarny i militarny. W przypadku zagrożeń militarnych mogą one przybrać postać zagrożeń kryzysowych oraz wojennych, to jest konfliktów zbrojnych o różnej skali – od działań zbrojnych poniżej progu klasycznej wojny, do mniej prawdopodobnego konfliktu na dużą skalę.

37. **NATO** pozostanie najważniejszym sojuszem polityczno-wojskowym oraz gwarantem bezpieczeństwa Polski. Kluczową sprawą jest utrzymanie przez Sojusz Północnoatlantycki pełnego spektrum zdolności wojskowych i politycznych oraz solidarności sojuszniczej, gwarantujących realizację jego podstawowej misji - kolektywnej obrony, a także podejmowanie innych zadań wynikających z ewolucji jego otoczenia.

38. **Unia Europejska** i rozwijana w jej ramach Wspólna Polityka Bezpieczeństwa i Obrony (WPBiO) będą stanowiły istotny czynnik bezpieczeństwa Polski. Dalszy rozwój WPBiO zależy od postępu procesów integracyjnych w Unii Europejskiej, intensyfikacji współdziałania UE i NATO, politycznej woli budowy zdolności obronnych oraz aktywnego zaangażowania operacyjnego UE w swoim sąsiedztwie. Ważne jest dążenie do rozwijania w ramach Unii Europejskiej współpracy w zakresie urzeczywistniania Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, w szczególności w obszarze wymiaru sprawiedliwości i spraw wewnętrznych. W interesie Polski jest ambitne podejście do tych wyzwań.

39. Utrzymywanie się tendencji spadkowej wielkości **budżetów obronnych państw NATO i UE** będzie negatywnie wpływać na zdolności do działania obu organizacji. Szansą dla poprawy tego stanu może być wzmocnienie strategicznej i operacyjnej współpracy NATO i UE w sferze bezpieczeństwa.

40. **Reorientacja amerykańskiej polityki zagranicznej** w kierunku Azji i Pacyfiku oraz ewolucja priorytetów USA w sferze bezpieczeństwa międzynarodowego będą wpływały na stan relacji transatlantyckich. Istotne jest utrzymanie znaczącego i trwałego zaangażowania Stanów Zjednoczonych w sprawy bezpieczeństwa europejskiego, w ramach NATO i relacji dwustronnych. Ważne jest również odpowiednie zaangażowanie we współpracę transatlantycką ze strony państw europejskich, które powinny zwiększać swoją odpowiedzialność w sferze bezpieczeństwa oraz rozwijać adekwatne zdolności i zasoby.

41. Relacje **Rosji** z Zachodem pozostaną ważnym czynnikiem oddziałującym na bezpieczeństwo Polski, regionu i Europy. Odbudowywanie mocarstwowości Rosji kosztem jej otoczenia oraz nasilanie się jej konfrontacyjnej polityki, czego przykładem jest konflikt z Ukrainą, w tym aneksja Krymu, negatywnie rzutuje na stan bezpieczeństwa w regionie.

42. Zmiany zachodzące w sferze bezpieczeństwa zwiększają znaczenie współpracy regionalnej, zarówno w wymiarze politycznym, jak i obronnym. Pogłębiona kooperacja subregionów Europy w dziedzinie bezpieczeństwa, w tym obrony, pozostanie korzystna polityczne i gospodarczo. Nie może ona jednak zastąpić rozwiązań sojuszniczych i ogólnoeuropejskich w tym względzie.

43. Wyzwaniem dla europejskiej polityki bezpieczeństwa stają się procesy zachodzące w państwach **wschodniego sąsiedztwa UE,** połączone z silną polityczną, wojskową i gospodarczą presją Rosji realizującej własne interesy. Dotyczy to przede wszystkim stanu demokracji i kierunków transformacji ustrojowej, potencjału militarnego, procesów reintegracyjnych obejmujących między innymi sferę obronności, a także konfliktów lokalnych i regionalnych sprzyjających utrwalaniu stanu niestabilności w tym regionie. Korzystny byłby szeroki udział jego państw w procesach integracji europejskiej, umacniających bezpieczeństwo i wzajemne zaufanie, opartych o zasady poszanowania suwerenności państwowej i integralności terytorialnej.

44. Poważnym wyzwaniem dla bezpieczeństwa europejskiego jest także sytuacja w regionie Afryki Północnej i Bliskiego Wschodu, jak również utrzymujący się potencjał niestabilności na Bałkanach.

45. W sferze bezpieczeństwa kooperatywnego nadal istotną rolę odgrywa potencjał **Organizacji Bezpieczeństwa i Współpracy w Europie** jako forum dyskusji politycznych i praktycznych działań służących rozwiązywaniu sytuacji konfliktowych. OBWE dysponuje szerokim instrumentarium rozwiązywania sytuacji kryzysowych, ale jego faktyczna efektywność zależna jest od zaangażowania państw uczestniczących. Pogłębiające się podziały w Europie powodują, że w najbliższych latach nie należy spodziewać się poprawy funkcjonowania tej organizacji.

46. Negatywnym zjawiskiem jest **osłabienie reżimu kontroli zbrojeń konwencjonalnych i systemu środków budowy zaufania w Europie**, czy też instrumentalne wykorzystywanie zapisów dokumentów OBWE w tej dziedzinie w celu legitymizacji nierzadko intensywnej działalności wojskowej. Kryzys wokół *Traktatu o Konwencjonalnych Siłach Zbrojnych w Europie (Traktat CFE)* pozostaje nierozwiązany i należy zakładać, iż stan ten nie ulegnie zmianie w dłuższej perspektywie. Będzie to miało swoje negatywne konsekwencje dla bezpieczeństwa i wzajemnego zaufania na obszarze OBWE.

47. Znaczeni**e bezpieczeństwa w cyberprzestrzeni** będzie rosło, podobnie jak odpowiedzialność państw za jej ochronę i obronę. Istotne znaczenie dla zwiększenia poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni ma polityka organizacji i struktur współpracy międzynarodowej, w pracach których Polska uczestniczy oraz współpraca dwustronna z wybranymi państwami, w szczególności z państwami NATO i UE.

48. **Starzenie się ludności** państw europejskich będzie powodowało obciążenia dla finansów publicznych. Zapewnienie zastępowalności pokoleń wymusza na Unii Europejskiej, w tym i na Polsce, wypracowanie wspólnych rozwiązań dotyczących migracji, doskonalenie standardów w zakresie polityki rodzinnej państw członkowskich, a także upowszechnienie polityki aktywnego i zdrowego starzenia. W interesie Polski jest, aby polityka migracyjna UE nie dyskryminowała państw Partnerstwa Wschodniego i umożliwiała napływ wysoko wykwalifikowanych pracowników.

49. Wskutek zależności państw Unii Europejskiej od importu surowców energetycznych, niezbędne będzie zapewnienie **bezpieczeństwa energetycznego** poprzez nieprzerwane oraz zdywersyfikowane źródła dostaw gazu ziemnego i ropy naftowej. Wyzwaniem będą również skutki ograniczenia transportu ropy naftowej przez terytorium Polski do państw Europy Środkowej, podobnie jak importu tego surowca do Polski przy wykorzystaniu istniejącej infrastruktury. Szansą będzie budowa wspólnego europejskiego rynku energii, utrzymanie solidarnych zachowań państw członkowskich, służących stworzeniu jednolitych reguł i instrumentów podnoszących bezpieczeństwo energetyczne. Wyzwaniem dla Polski będzie zapewnienie efektywnych warunków instytucjonalnych i prawnych dla poszukiwań i eksploatacji surowców ze złóż niekonwencjonalnych oraz dla rozwoju energetyki jądrowej, której znaczna część cyklu paliwowego zlokalizowana jest na obszarze UE, a wykorzystywany na jej potrzeby uran znajduje się głównie w krajach stabilnych politycznie.

50. Zachowanie **różnorodności biologicznej** jest ważnym celem polityki europejskiej. Jednym z narzędzi jego realizacji jest sieć obszarów Natura 2000, chroniąca gatunki i siedliska o znaczeniu wspólnotowym. Istotne jest włączanie problematyki różnorodności biologicznej do innych polityk i uwzględnienie kosztów jej utraty w rachunku ekonomicznym.

2.3. Wymiar krajowy

51. Pogarszająca się **sytuacja demograficzna**, spowodowana malejącym przyrostem naturalnym i emigracją zarobkową, staje się coraz poważniejszym wyzwaniem rozwojowym Polski. Wiąże się to z rozlicznymi zagrożeniami, w tym związanymi z niedoborem siły roboczej, znacznym obciążeniem dla systemu ubezpieczeń społecznych oraz z koniecznością zapewnienia warunków dla wydłużenia aktywności zawodowej i społecznej osób starszych.

52. Barierą dla dalszego rozwoju jest także utrzymujące się zjawisko długotrwałego bezrobocia, ubóstwa i wykluczenia społecznego, a co za tym idzie **rozwarstwienia społecznego** i nierównego dostępu do dóbr i usług. Szansą na zwiększenie spójności społecznej będą działania aktywizujące, umożliwiające powszechne uczestnictwo w różnych sferach życia społeczno-gospodarczego.

53. **Bezpieczeństwo zdrowotne** obywateli współkształtuje bezpieczeństwo narodowe. Wpływają na nie nasilające się zmiany demograficzne, zmiany warunków środowiskowych oraz rozwój nowych technologii.

54. Utrzymywać się będą wyzwania dla **bezpieczeństwa powszechnego i porządku publicznego**, w tym te związane z ochroną ludności, bezpieczeństwem imprez masowych i ruchu drogowego oraz przestępczością zorganizowaną, gospodarczą, narkotykową i handlem ludźmi.

55. Międzynarodowy charakter **terroryzmu** oraz intensywność jego przejawów sprawiają, że Polska nie jest wolna od tego typu zagrożeń. Szczególnie niebezpieczne mogą okazać się pojedyncze osoby lub małe grupy osób wykorzystujące metody terroru jako narzędzia do realizowania własnych celów o podłożu politycznym, społecznym, ekonomicznym lub religijnym.

56. Rosnąca pozycja Polski na arenie międzynarodowej oraz członkostwo w NATO i UE wpływają na zwiększone zainteresowanie **obcych służb wywiadowczych** naszym krajem. Ewentualne nieuprawnione ujawnienie czy kradzież informacji niejawnych oraz innych chronionych prawem danych może spowodować straty dla bezpieczeństwa narodowego i interesów Rzeczypospolitej Polskiej.

57. **Bezpieczne funkcjonowanie systemu teleinformatycznego Rzeczypospolitej Polskiej** jest warunkiem niezakłóconego działania całego państwa. Wyzwaniem pozostaje zapewnienie dostępności, integralności i poufności danych przetwarzanych w systemach teleinformatycznych administracji publicznej oraz brak jednolitych zabezpieczeń teleinformatycznych. Istotne znaczenie z punktu widzenia bezpieczeństwa ma niewystarczająca wiedza użytkowników o zagrożeniach w cyberprzestrzeni oraz konieczność rozwiązania dylematu pomiędzy wolnością osobistą i ochroną praw jednostki, a stosowaniem środków służących zachowaniu bezpieczeństwa państwa.

58. **Korupcja** stanowi barierę dla dalszego rozwoju Polski i wyzwanie dla jej bezpieczeństwa ekonomicznego. Obszary szczególnie nią zagrożone to: infrastruktura, informatyzacja administracji publicznej, wykorzystywanie środków unijnych, służba zdrowia, obronność, energetyka oraz ochrona środowiska.

59. **Bezpieczny system finansowy**, oparty na zrównoważonych w średnim okresie finansach publicznych, z instytucjami finansowymi zbudowanymi adekwatnie do wyzwań czasu, jest jednym z najważniejszych instrumentów stabilnego rozwoju państwa.

60. Wyzwaniem dla bezpieczeństwa narodowego jest uzależnienie krajowej gospodarki od dostaw surowców energetycznych z jednego źródła oraz wahania cen tych surowców spowodowane wydarzeniami na rynkach międzynarodowych. Na sektor energetyczny coraz silniej będzie oddziaływała polityka regulacyjna UE, tworząc wyzwania finansowe oraz ograniczenia swobody działania w sferze energetycznej. Do poprawy **bezpieczeństwa energetycznego** przyczyni się dywersyfikacja dróg i źródeł dostaw surowców, z wykorzystaniem złóż niekonwencjonalnych, źródeł wytwarzania, między innymi w oparciu o energetykę jądrową, a także zapewnienie stabilności dostaw energii poprzez rozwój infrastruktury wytwórczej i sieciowej.

61. Niezadowalająca konkurencyjność **polskiej gospodarki** jest wyzwaniem dla bezpieczeństwa. Innowacyjność, rozwój oparty na wiedzy, e-biznes oraz tworzenie korzystnych warunków organizacyjnych, finansowych i prawnych dla działalności gospodarczej stwarzają szansę szybkiej poprawy sytuacji.

62. **Przemysł** pozostaje kluczowym czynnikiem budowania dobrobytu i mocnej pozycji Polski na arenie europejskiej i międzynarodowej. Wyzwaniem będzie utrzymanie silnej krajowej bazy przemysłowej. W warunkach nowoczesnej gospodarki rośnie udział sektora usług w tworzeniu PKB. Konkurencyjna, nowoczesna i przyjazna środowisku gospodarka umożliwi obniżenie cen i kosztów oraz tworzenie nowych, lepszych dóbr i usług.

63. **Dekapitalizacja majątku narodowego**, w szczególności infrastruktury przemysłowej, energetycznej, transportowej oraz mieszkaniowej, może powodować wzrost zagrożenia katastrofami o podłożu technicznym. Szczególną uwagę należy zwrócić na jej elementy zaliczane do infrastruktury krytycznej.

ROZDZIAŁ III. KONCEPCJA DZIAŁAŃ STRATEGICZNYCH. STRATEGIA OPERACYJNA

64. Interesy narodowe i cele strategiczne Polski w powiązaniu z diagnozą środowiska bezpieczeństwa narodowego określają priorytety polityki bezpieczeństwa i obronnej. Wskazują one na potrzebę zrównoważonego umiędzynarodowienia i samodzielności w zakresie bezpieczeństwa Polski, w tym zwiększenia strategicznej odporności kraju na różnego rodzaju zagrożenia.

65. Główny kierunek działań strategicznych w tym zakresie określają trzy priorytety polityki bezpieczeństwa, do których należą:

- **zapewnienie gotowości i demonstracja determinacji do działania w sferze bezpieczeństwa i obrony** oraz wzmocnienie narodowych zdolności obronnych, ze szczególnym traktowaniem tych obszarów bezpieczeństwa narodowego, w których sojusznicze (wspólne) działania mogą być utrudnione (sytuacje trudnokonsensusowe);

- **wspieranie procesów służących wzmocnieniu zdolności NATO do kolektywnej obrony, rozwój Wspólnej Polityki Bezpieczeństwa i Obrony UE, umacnianie strategicznych partnerstw** (w tym z USA) oraz strategicznych relacji z partnerami w regionie;

- **wspieranie i selektywny udział w działaniach społeczności międzynarodowej**, realizowanych na podstawie norm prawa międzynarodowego, mających na celu zapobieganie powstawaniu nowych źródeł zagrożeń, reagowanie na zaistniałe kryzysy oraz przeciwdziałanie ich rozprzestrzenianiu się.

66. W ramach pierwszego priorytetu Polska koncentruje wysiłki strategiczne głównie na zapewnieniu bezpieczeństwa własnych obywateli oraz terytorium państwa, wsparciu obrony państw sojuszniczych zgodnie z przyjętymi umowami międzynarodowymi, a następnie na udziale w reagowaniu na zagrożenia poza terytorium sojuszniczym. Podstawowy warunek tworzy społeczne przyzwolenie oraz polityczne porozumienie co do **nadrzędnego traktowania spraw bezpieczeństwa narodowego** w polityce państwa. Determinacja, zdolność i gotowość do działania, oparte na szerokim konsensusie politycznym, wzmacniają siłę Polski w stosunkach międzynarodowych, konieczną zarówno do przyciągania sojuszników i partnerów, jak i odstraszania potencjalnych przeciwników. Umożliwiają też skuteczne reagowanie na presję czy szantaż polityczno-militarny. Ważnymi instrumentami gwarantującymi społeczne i polityczne porozumienie w sprawach bezpieczeństwa są: edukacja obywatelska, dialog społeczny, współpraca parlamentarna, a także Rada Bezpieczeństwa Narodowego.

67. W ramach drugiego priorytetu Polska będzie koncentrowała się na działaniach służących **konsolidacji NATO wokół funkcji obronnej**, w tym strategicznemu wzmocnieniu wschodniej flanki Sojuszu. Zmierzają one do rozwoju praktycznych mechanizmów kolektywnej obrony, a zwłaszcza adekwatne do zagrożeń kształtowanie zdolności wojskowych. Duże znaczenie dla bezpieczeństwa Polski ma także rozwój i spójność polityczna Unii Europejskiej. Działania państwa polskiego będą ukierunkowane na **pogłębianie procesów integracyjnych UE w dziedzinie bezpieczeństwa**, tak aby dysponowała ona adekwatnym potencjałem

bezpieczeństwa, w tym obronnym. W interesie Polski jest poprawa **strategicznej współpracy między NATO a UE** - wzmocnienie spójności politycznej oraz zwiększenie skuteczności w działaniu. Pośród strategicznych partnerstw Polski priorytetowe znaczenie ma **współpraca ze Stanami Zjednoczonymi Ameryki**. Polska będzie zabiegała o jak najszerszą obecność wojskową USA w Europie, w tym w Polsce oraz będzie wspierała działania na rzecz zachowania amerykańskich gwarancji dla bezpieczeństwa Europy. Będzie także aktywnie działała na rzecz wzmacniania podmiotowości **państw Europy Wschodniej**, zwłaszcza objętych inicjatywą Partnerstwa Wschodniego UE. Z sąsiadami Polski rozwijane będą stosunki z wykorzystaniem różnych form współpracy. W relacjach z Federacją Rosyjską istotne będzie rozwiązywanie spraw trudnych z uwzględnieniem standardów prawa międzynarodowego. Punktem wyjścia dla kształtowania stosunków NATO z Rosją powinny być: analiza sojuszniczych interesów bezpieczeństwa, przestrzeganie norm prawa międzynarodowego oraz zasady pragmatyzmu i wzajemności. Rozwijana będzie współpraca regionalna w ramach Grupy Wyszehradzkiej. Konieczne będzie intensyfikowanie relacji z państwami o rosnącej pozycji międzynarodowej.

68. Realizacja trzeciego priorytetu wymaga podjęcia działań na rzecz wzmocnienia **ONZ**, kontynuacji starań o dokonanie przeglądu norm prawa międzynarodowego oraz wzmacniania skuteczności reżimów i regulacji w obszarze kontroli zbrojeń i rozbrojenia, w tym środków budowy zaufania i bezpieczeństwa. W wymiarze regionalnym istnieje potrzeba odbudowy znaczenia **OBWE**, choć proces ten wymaga konstruktywnego podejścia wszystkich państw członkowskich. Ważną formą udziału w działaniach społeczności międzynarodowej jest uczestnictwo w operacjach poza granicami kraju. Działania wojskowe powinny być wzmacniane poprzez zaangażowanie cywilne, w tym poprzez pomoc rozwojową.

69. Zgodnie z przyjętymi priorytetami Polska organizuje i prowadzi następujące rodzaje działań strategicznych w sferze bezpieczeństwa: działania obronne, ochronne oraz w sferze bezpieczeństwa społecznego i gospodarczego.

3.1. Działania obronne

70. Istotą działań obronnych jest stałe utrzymywanie gotowości do skutecznego reagowania na zagrożenia dla niepodległości i nienaruszalności terytorialnej Rzeczypospolitej Polskiej. Do działań uzupełniających należy aktywne wykorzystywanie szans i uprzedzające redukowanie ryzyk w dziedzinie bezpieczeństwa, między innymi poprzez udział w międzynarodowych wysiłkach na rzecz ograniczania źródeł zagrożeń, w tym w międzynarodowych operacjach bezpieczeństwa. Służą temu: działania dyplomatyczne na rzecz bezpieczeństwa, działania wojskowe, działania wywiadowcze i kontrwywiadowcze w sferze obronnej oraz funkcjonowanie naukowo-przemysłowego potencjału obronnego.

71. **Działania dyplomatyczne** służą zapewnieniu korzystnych warunków międzynarodowych, możliwie najpełniej gwarantujących realizację szeroko pojętych interesów Rzeczypospolitej Polskiej. Stałym kierunkiem aktywności polskiej dyplomacji w obszarze bezpieczeństwa są działania służące wzmacnianiu wiarygodności i skuteczności kolektywnej obrony oraz siły odstraszania Sojuszu Północnoatlantyckiego, wsparciu dla usprawnienia WPBiO UE w wymiarze polityczno-strategicznym, instytucjonalnym i operacyjnym oraz poprawie strategicznej współpracy między NATO a UE. Równie ważnym zadaniem dyplomacji jest kształtowanie efektywnej współpracy dwustronnej i wielostronnej, w tym: dalsze wzmacniane ugrupowań regionalnych, które współtworzy Polska - głównie Trójkąta Weimarskiego i Grupy Wyszehradzkiej; rozwijanie potencjału współpracy między innymi z Litwą, Łotwą, Estonią i państwami nordyckimi oraz Rumunią; poszerzenie spektrum współpracy dwustronnej ze Stanami Zjednoczonymi Ameryki, przy jednoczesnej intensyfikacji współpracy polityczno-wojskowej; wspieranie reform państw Europy Wschodniej, zwłaszcza w ramach Partnerstwa Wschodniego UE; kształtowanie stosunków z Rosją na zasadach wzajemności, przejrzystości oraz respektowania suwerenności państw sąsiednich*;* rozszerzanie relacji partnerskich ze wschodzącymi mocarstwami, w tym dialog w sprawach bezpieczeństwa.

72. Istotnym obszarem zainteresowania jest kontrola zbrojeń konwencjonalnych i system środków budowy zaufania w Europie. Kontynuowane będą działania na rzecz przełamania impasu wokół *Traktatu CFE,* jego wzmocnienia, modernizacji i rozbudowy. Konieczne jest utrzymanie i umacnianie aktywnej pozycji Polski w systemie nierozprzestrzeniania broni masowego rażenia. Dotyczy to także ograniczenia ryzyka rozwoju nowych dziedzin proliferacji (np. poprzez Inicjatywę na Rzecz Nieproliferacji Broni Masowego Rażenia - PSI).

73. **Działania w sferze militarnej** ukierunkowane są na utrzymywanie i demonstrowanie wszechstronnej gotowości państwa do skutecznego reagowania na militarne zagrożenia dla niepodległości i integralności terytorialnej Polski. Zadania w tym zakresie wykonują przede wszystkim Siły Zbrojne RP, które są gotowe do realizacji trzech rodzajów misji: zagwarantowania obrony państwa i przeciwstawienia się agresji zbrojnej; wspierania podsystemów ochronnych w zakresie bezpieczeństwa wewnętrznego i pomocy społeczeństwu; udziału w procesie stabilizacji sytuacji międzynarodowej, w tym w międzynarodowych działaniach z dziedziny zarządzania kryzysowego. W misji obrony państwa mieści się również wypełnianie funkcji militarnego odstraszania, poprzez demonstrowanie gotowości do obrony siłami utrzymywanymi w czasie pokoju oraz gotowości do ich mobilizacyjnego rozwinięcia w razie wojny.

74. Główne zadania Sił Zbrojnych RP, nadające kierunek działalności planistycznej i szkoleniowej w czasie pokoju, dotyczą zapewnienia zdolności państwa do: obrony i przeciwstawienia się agresji; utrzymywania gotowości do realizacji zadań związanych z obroną i ochroną nienaruszalności granic; prowadzenia strategicznej operacji obronnej na terytorium Rzeczypospolitej Polskiej; udziału w działaniach antyterrorystycznych w kraju i poza granicami; udziału w operacji obronnej poza obszarem państwa odpowiednio do zobowiązań sojuszniczych w ramach artykułu 5 Traktatu Północnoatlantyckiego; prowadzenia działalności rozpoznawczej i wywiadowczej. W operacji obronnej na terytorium kraju szczególne zadania przewidzieć należy dla oddziałów i pododdziałów Wojsk Specjalnych oraz formacji Narodowych Sił Rezerwowych.

75. W celu wypełnienia misji związanej ze wspieraniem podsystemów ochronnych w zakresie bezpieczeństwa wewnętrznego i pomocy społeczeństwu Siły Zbrojne RP utrzymują zdolność do realizacji zadań polegających na: monitorowaniu i ochronie przestrzeni powietrznej oraz wsparciu ochrony granicy państwowej na lądzie i morzu; prowadzeniu działalności rozpoznawczej i wywiadowczej; monitorowaniu skażeń promieniotwórczych, chemicznych i biologicznych na terytorium kraju; oczyszczaniu terenu z materiałów wybuchowych i przedmiotów niebezpiecznych pochodzenia wojskowego; prowadzeniu działań poszukiwawczo-ratowniczych; pomocy władzom państwowym, administracji publicznej oraz społeczeństwu w reagowaniu na zagrożenia (sytuacje kryzysowe) oraz likwidacji ich skutków. W tym ostatnim zadaniu szczególną rolę spełniać powinny formacje Narodowych Sił Rezerwowych, wydzielane w razie potrzeby do użycia przez wojewodów.

76. Uczestnictwo w działaniach na rzecz stabilizacji sytuacji międzynarodowej oraz w międzynarodowych misjach i operacjach zarządzania kryzysowego wymaga utrzymywania przez Siły Zbrojne RP adekwatnych sił i środków wspierających udział w różnych typach operacji i misji zarządzania kryzysowego (pokojowych, reagowania kryzysowego, pomocy humanitarnej) prowadzonych przez NATO, UE, ONZ oraz innych operacjach wynikających z porozumień międzynarodowych, a także współpracy wojskowej w zakresie rozwoju i stosowania środków budowy zaufania i bezpieczeństwa.

77. Cyberprzestrzeń stała się kolejnym środowiskiem walki zbrojnej. Siły Zbrojne RP muszą dysponować zdolnościami defensywnymi i ofensywnymi w tej sferze, tak aby realizować funkcję odstraszania potencjalnego przeciwnika. W szczególności muszą być one gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na większą skalę w razie cyberkonfliktu lub cyberwojny.

78. **Działania służb specjalnych w sferze obronnej**. Podstawową misją służb wywiadu w sferze obronnej jest uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie informacji organom państwa odpowiedzialnym za bezpieczeństwo narodowe o istniejących i potencjalnych zagrożeniach Rzeczypospolitej Polskiej, jej interesów oraz obywateli. Działania wywiadowcze obejmują także: identyfikowanie i monitorowanie szans oraz ryzyk dla bezpieczeństwa narodowego; wspieranie Sił Zbrojnych RP uczestniczących w operacjach poza granicami kraju; monitorowanie międzynarodowego obrotu bronią oraz proliferacji broni masowego rażenia i środków jej przenoszenia; obserwację działań związanych z polityką energetyczną i surowcową; zwiększanie własnych możliwości poprzez współpracę z sojusznikami oraz koalicjantami. Zadaniem służb kontrwywiadu w sferze obronnej jest przeciwdziałanie: szpiegostwu, zamachom na jednostki wojskowe oraz obiekty lub urządzenia o znaczeniu obronnym, korupcji w obszarze produkcji dla obronności państwa i naruszeniom ochrony informacji niejawnych, jak również szeroko pojętego bezpieczeństwa informacyjnego. Istotnym zadaniem w tym obszarze jest także zapewnienie bezpieczeństwa badań naukowych i prac rozwojowych zlecanych przez Siły Zbrojne RP oraz inne jednostki resortu obrony narodowej, a także zabezpieczanie produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym.

79. **Produkcja obronna.** Polski przemysłowy potencjał obronny - istotny element gospodarczej sfery bezpieczeństwa - powinien być w maksymalnym stopniu angażowany w proces modernizacji technicznej Sił Zbrojnych RP, a w szczególności w realizowane przez resort obrony narodowej priorytetowe programy modernizacyjne. Działania te powinny być uzupełnione przez mechanizmy wspierania rozwoju podmiotów sektora obronnego, w tym małych i średnich przedsiębiorców oraz dążenie do wyrównywania różnic w rozwoju produkcji i potencjału obronnego w skali europejskiej pozwalającej na zwiększenie konkurencyjności polskiego przemysłowego potencjału obronnego.

3.2. Działania ochronne

80. Istotą działań ochronnych jest zapewnienie warunków dla utrzymywania ładu konstytucyjnego, wewnętrznej stabilności państwa, bezpieczeństwa powszechnego i porządku publicznego, zarówno wspólnych, jaki i indywidualnych zasobów materialnych i niematerialnych, a także funkcjonowania infrastruktury krytycznej. Działaniem uzupełniającym powinno być uczestnictwo w promowaniu na arenie międzynarodowej oraz krzewienie w społeczeństwie polskim zasad i świadomości należytego korzystania z praw i wolności człowieka i obywatela.

81. Nadrzędnym celem działań **wymiaru sprawiedliwości** jest eliminowanie źródeł zagrożeń dla swobody korzystania z praw i wolności oraz konsekwentne ściganie i karanie sprawców ich naruszeń. W tym zakresie szczególne znaczenie ma zapewnienie przez państwo sprawnego funkcjonowania sądów i prokuratury, terminowe prowadzenie postępowań i rozstrzyganie spraw oraz zagwarantowanie skutecznego wykonania orzeczeń. Ważnym elementem zapewnienia bezpieczeństwa obywatelom jest również zagwarantowanie bezpieczeństwa obrotu gospodarczego, dzięki uproszczeniu i uelastycznieniu procedur prawnych. Konstytucyjne gwarancje ochrony praw i wolności będą w pełni realizowane, gdy instytucje wymiaru sprawiedliwości staną się powszechnie dostępne, szybkie w działaniu oraz przyjazne dla obywateli.

82. **Osłona kontrwywiadowcza** ukierunkowana jest na ochronę porządku konstytucyjnego i demokratycznego ustroju przed naruszeniami stabilności państwa oraz operacyjne rozpoznawanie zagrożeń dla bezpieczeństwa Polski, wynikających z działalności obcych służb specjalnych. Do głównych zadań kontrwywiadu w tym zakresie należy zaliczyć: skuteczne rozpoznawanie potencjalnych i realnych zagrożeń oraz zapobieganie im za pomocą dostępnych metod operacyjnych i procesowych; bieżący monitoring i analizę sytuacji w obszarze zidentyfikowanych zagrożeń dla bezpieczeństwa państwa; prowadzenie działań profilaktycznych, szczególnie w zakresie ochrony informacji niejawnych; koordynację działań

i współpracy z innymi komponentami systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej oraz podmiotami zagranicznymi i międzynarodowymi zgodnie z zobowiązaniami sojuszniczymi.

83. **Przeciwdziałanie i zwalczanie terroryzmu i ekstremizmu.** Globalny zasięg i skala zjawiska terroryzmu stanowią poważne wyzwanie dla większości organów międzynarodowych i państwowych. Do najważniejszych zadań w zakresie przeciwdziałania i zwalczania terroryzmu i ekstremizmu należą: rozpoznawanie i monitorowanie zagrożeń terrorystycznych dla Polski i jej obywateli w kraju i za granicą; wykrywanie i neutralizacja zagrożeń terrorystycznych, w tym fizyczne zwalczanie terroryzmu; eliminowanie źródeł finansowania terroryzmu; ściganie karne sprawców zagrożeń terrorystycznych, zgodnie z prawem krajowym oraz obowiązującymi Polskę normami prawa międzynarodowego; rozpoznawanie źródeł terroryzmu i symptomów radykalizacji zachowań i zapobieganie im; współpraca międzynarodowa dwu- i wielostronna na szczeblu politycznym, operacyjnym, analitycznym i prawno-karnym w obszarze zwalczania terroryzmu; profilaktyka antyterrorystyczna, rozwój partnerstwa publiczno-prywatnego, polityka medialna i informowanie społeczeństwa o potencjalnych zagrożeniach, edukacja społeczna. Istotnym elementem działań jest też poprawa bazy prawnej i implementacja dokumentów międzynarodowych do prawa krajowego.

84. **Zapewnienie bezpieczeństwa Polski w cyberprzestrzeni,** w tym bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, to jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa. Powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Szczególnie ważna jest: współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej; prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni; wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie; rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców; prowadzenie walki informacyjnej w cyberprzestrzeni; współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych.

85. Bezpieczeństwo informacyjne, w tym **ochrona informacji niejawnych**, to jeden z najważniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa. Strategiczne zadania w tym zakresie obejmują: zapewnienie bezpieczeństwa informacyjnego państwa poprzez zapobieganie uzyskaniu nieuprawnionego dostępu do informacji niejawnych i ich ujawnieniu; zapewnianie personalnego, technicznego i fizycznego bezpieczeństwa informacji niejawnych; akredytację systemów teleinformatycznych służących przetwarzaniu tych informacji; zapewnienie realizacji funkcji krajowej władzy bezpieczeństwa w celu umożliwienia międzynarodowej wymiany informacji niejawnych.

86. Niezwykle istotne jest zapewnienie warunków **ochrony infrastruktury krytycznej**. Infrastruktura ta obejmuje kluczowe systemy i elementy zapewniające bezpieczeństwo państwa i jego obywateli oraz sprawne funkcjonowanie organów administracji publicznej, instytucji i przedsiębiorców. Ochrona infrastruktury krytycznej jest obowiązkiem operatorów i właścicieli, którzy są wspierani przez potencjał administracji publicznej. W Polsce wdrażane jest nowatorskie podejście w tym zakresie, bazujące na zasadach współodpowiedzialności zainteresowanych stron, rozbudowanej współpracy i wzajemnego zaufania. Działania państwa polegają na ewentualnym uruchomieniu sytemu zarządzania kryzysowego na wypadek zakłócenia funkcjonowania infrastruktury krytycznej, a także na podnoszeniu świadomości, wiedzy i kompetencji oraz propagowaniu współpracy w tym obszarze.

87. Podstawą **utrzymania bezpieczeństwa i porządku publicznego** na właściwym poziomie jest skuteczne zapobieganie ich naruszeniom, a także wykrywanie przestępstw i wykroczeń

godzących w życie, zdrowie i mienie obywateli, jak również interesy państwa. Zadania realizowane w tym zakresie dotyczą różnego rodzaju czynów zabronionych, w tym zarówno przestępczości pospolitej, jak i zorganizowanej o charakterze ekonomicznym, narkotykowym i kryminalnym. Przedmiotowe działania pozostaną ukierunkowane na zwiększenie efektywności w zakresie przeciwdziałania i wykrywania przestępstw i wykroczeń, nieuchronności karania ich sprawców, odzyskiwania utraconego mienia oraz minimalizowania strat budżetu państwa. Istotną rolę odgrywać będzie również koordynacja działań i współpraca z innymi podmiotami systemu bezpieczeństwa narodowego, w tym z właściwymi organami administracji publicznej oraz wewnętrznymi służbami ochrony, a także partnerami zagranicznymi i międzynarodowymi. Najważniejszą służbą realizującą zadania z tego zakresu jest Policja, właściwa w zakresie ochrony życia i zdrowia oraz mienia przed bezprawnymi zamachami naruszającymi te dobra.

88. **Zapewnienie bezpieczeństwa powszechnego (ratownictwo i ochrona ludności).** Podstawowym zadaniem ochronnym są działania związane z ratowaniem życia, zdrowia, mienia i środowiska przed klęskami żywiołowymi lub spowodowanymi działalnością człowieka oraz innymi miejscowymi zagrożeniami. Wiodącą rolę w tym zakresie odgrywa Państwowe Ratownictwo Medyczne oraz Państwowa Straż Pożarna, która jako główny element krajowego systemu ratowniczo-gaśniczego działa na rzecz rozpoznawania zagrożeń, przygotowania i prowadzenia działań ratowniczych (także w sytuacjach kryzysowych, takich jak katastrofy i wypadki komunikacyjne, budowlane, chemiczne i zdarzenia radiacyjne). Ważnym wsparciem w tym zakresie jest współpraca ze wszystkimi służbami i podmiotami ratowniczymi, uwzględniająca również podmioty niezaliczone do sektora finansów publicznych (w tym organizacje pozarządowe, takie jak ochotnicze straże pożarne, podmioty uprawnione do ratownictwa górskiego i wodnego), a ustawowo uprawnione do realizowania działań z zakresu ratownictwa w Polsce.

89. **Ochrona granicy państwowej.** Zasadnicze działania w zakresie zapewnienia nienaruszalności i bezpieczeństwa granic wykonują Straż Graniczna, Służba Celna, Urząd do Spraw Cudzoziemców oraz Siły Zbrojne RP. Do zadań realizowanych przez te służby i organy należy: ochrona terytorium Rzeczypospolitej Polskiej przed nielegalnym przepływem towarów i osób oraz wprowadzaniem substancji i materiałów niebezpiecznych; organizowanie i prowadzenie kontroli ruchu granicznego w sposób zapewniający płynność ruchu na granicach, zwalczanie przestępczości transgranicznej oraz przestępczości z udziałem cudzoziemców; ochrona obszaru celnego UE, w tym zgodność z prawem przywozu i wywozu towarów; utrzymanie przejść granicznych; regulacja i kontrola legalności pobytu cudzoziemców na terytorium kraju oraz ich zatrudnienia; ochrona polskiej przestrzeni powietrznej; prowadzenie akcji ratunkowych na morskim odcinku granicy państwowej.

90. Działania z zakresu **ochrony najważniejszych organów władzy i administracji publicznej** realizowane są przez Biuro Ochrony Rządu (BOR), zarówno na terenie kraju, jak i poza jego granicami. Do głównych zadań BOR należy ochrona osób i obiektów ważnych ze względu na interes państwa oraz delegacji państw obcych przebywających w Polsce, polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych. Priorytetem jest zapewnienie maksymalnej ochrony polskich placówek i przedstawicielstw w miejscach występowania dużych napięć społecznych czy rejonach o wysokim poziomie zagrożenia terroryzmem.

91. Do głównych zadań z zakresu **zarządzania kryzysowego** należą: przygotowanie administracji publicznej do działań w sytuacjach kryzysowych, przeciwdziałanie ich powstawaniu, a także sprawna wymiana informacji, podejmowanie decyzji i koordynacja działań, efektywne wykorzystanie sił i środków państwa (również w fazie reagowania i odbudowy), współpraca ze strukturami zarządzania kryzysowego NATO i UE, współpraca dwustronna i międzynarodowa, w szczególności z państwami regionu.

92. Skuteczne zarządzanie rozwojem kraju oraz ochrona praw obywateli wymagają **przeciwdziałania i zwalczania zjawisk korupcyjnych i korupcjogennych**. Zadania strategiczne

w tym obszarze polegają na zwalczaniu korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych; skutecznym wykrywaniu przestępstw korupcyjnych i ściganiu ich sprawców; wdrożeniu efektywnych mechanizmów walki z korupcją w administracji publicznej; realizacji postanowień rządowych programów przeciwdziałania korupcji; zwiększeniu świadomości publicznej i promocji etycznych wzorców postępowania; realizacji zobowiązań międzynarodowych Polski dotyczących prewencji i edukacji antykorupcyjnej.

93. **Ochrona zdrowia** obejmuje rozpoznawanie i przeciwdziałanie zagrożeniom bezpieczeństwa zdrowotnego, w tym związanych z rozwojem współczesnej cywilizacji, a także ratowanie życia i zdrowia ludności. Zapewnienie właściwego poziomu świadczeń zdrowotnych jest nadrzędnym zadaniem realizowanym przez szereg organów i inspekcji oraz podmioty lecznicze, zaangażowane w proces świadczenia usług medycznych.

3.3. Działania społeczne w sferze bezpieczeństwa

94. Istotą działań społecznych w sferze bezpieczeństwa jest stworzenie bezpiecznych warunków godziwego życia obywateli oraz rozwoju duchowego i materialnego narodu. Ochrona dziedzictwa narodowego, w tym zapewnienie możliwości jego bezpiecznego rozwoju, zwłaszcza w sferze ekonomicznej, społecznej i intelektualnej oraz niematerialne wsparcie systemu bezpieczeństwa narodowego należą do kluczowych działań.

95. **Ochrona i umacnianie tożsamości narodowej.** Ważnym zadaniem państwa jest zachowanie tożsamości narodowej poprzez pielęgnowanie kultury narodowej oraz ciągłości historycznej i pokoleniowej. Konieczna jest nie tylko ochrona dziedzictwa kulturowego i tożsamości narodowej, ale też wydobywanie tkwiącego w nich potencjału rozwoju i budowy nowoczesnego państwa. Działania w tym zakresie będą więc ukierunkowane na zapewnienie powszechnego i równego dostępu do kultury, aktywizację kapitału społecznego, a w jego ramach wzmacnianie postaw patriotycznych oraz aktywnego i świadomego obywatelstwa. Służyć temu będzie ochrona samego dziedzictwa narodowego i jego cyfryzacja, otwarty dostęp do jego zasobów, rozwój edukacji obywatelskiej i kulturalnej w kształceniu ogólnym oraz wsparcie potencjału stowarzyszeń i organizacji pozarządowych zajmujących się tą problematyką.

96. **Edukacja dla bezpieczeństwa** obejmuje działalność służącą zdobywaniu przez obywateli wiedzy i umiejętności z zakresu bezpieczeństwa. Realizowana jest przez szkolnictw o powszechne i wyższe, centralne i lokalne instytucje państwowe oraz stowarzyszenia i organizacje pozarządowe. Priorytetowe znaczenie ma podnoszenie świadomości społecznej w kwestii rozumienia zagrożeń dla bezpieczeństwa oraz kształtowanie kompetencji pozwalających w sposób celowy i racjonalny reagować na nie. Istotne jest także zwiększanie efektywności działania administracji publicznej w sprawach bezpieczeństwa poprzez ustawiczne podnoszenie kwalifikacji i zdolności do skutecznego reagowania na zagrożenia.

97. **Działania mediów na rzecz bezpieczeństwa.** Strategicznym zadaniem w tym sektorze bezpieczeństwa jest zacieśnianie współdziałania administracji i służb z mediami, którego celem jest budowanie i pogłębianie świadomości społecznej w zakresie odpowiedniego reagowania na pojawiające się zagrożenia. Ponadto należy położyć nacisk na prowadzenie działalności o charakterze edukacyjnym, mającej na celu szerzenie wiedzy na temat odpowiedniego identyfikowania zagrożeń i skutecznego reagowania w takich sytuacjach.

98. **Przeciwdziałanie zagrożeniom dla bezpieczeństwa demograficznego.** Demografia stanowi istotny składnik bezpieczeństwa narodowego, wpływający na wszystkie aspekty jego potencjału. Strategicznym zadaniem w tym obszarze jest zahamowanie obecnych i prognozowanych niekorzystnych zmian demograficznych w Polsce. Istotne w tym zakresie jest tworzenie warunków sprzyjających zwiększaniu liczby urodzeń oraz wsparcie rodzin z dziećmi na utrzymaniu. Stanie się to możliwe dzięki umiejętnie prowadzonej polityce rodzinnej, rynku pracy oraz mieszkaniowej. Kluczowe będą też działania na rzecz ochrony osób starszych oraz odpowiednia polityka migracyjna.

99. **Zapewnienie bezpieczeństwa socjalnego** wymaga szeregu działań na rzecz poprawy integracji społecznej oraz zapewnienia dostępu do usług publicznych o odpowiednich standardach. Priorytetem polskiej polityki społecznej jest zmniejszanie ubóstwa i wykluczenia społecznego poprzez aktywizację, w szczególności na rynku pracy, osób wykluczonych i zagrożonych ubóstwem. Działania na rzecz zapobiegania rozwarstwieniu i wykluczeniu społecznemu będą wykorzystywały między innymi dobre praktyki wynikające ze współpracy instytucji pomocy społecznej oraz instytucji rynku pracy i ochrony zdrowia.

3.4. Działania gospodarcze w sferze bezpieczeństwa

100. Istotą działań gospodarczych w sferze bezpieczeństwa jest ochrona podmiotów i materialnych zasobów gospodarczego potencjału bezpieczeństwa narodowego przed zagrożeniami w czasie pokoju, kryzysu i wojny oraz wsparcie działania podsystemów operacyjnych systemu bezpieczeństwa narodowego.

101. **Wzmacnianie bezpieczeństwa finansowego.** W najbliższych latach najważniejszym zadaniem w obszarze bezpieczeństwa finansowego będzie wzmocnienie stabilności makroekonomicznej poprzez uzdrowienie finansów publicznych, zwiększenie stopy oszczędności i inwestycji oraz rozwój eksportu towarów i usług. Istotne jest też wzmocnienie nadzoru finansowego nad wszystkimi instytucjami świadczącymi usługi o charakterze bankowym.

102. **Zwiększanie bezpieczeństwa energetycznego.** Strategicznym zadaniem na rzecz bezpieczeństwa energetycznego jest uruchomienie wydobycia surowców energetycznych z krajowych złóż niekonwencjonalnych, rozwój infrastruktury sieciowej i wytwórczej w oparciu o paliwa węglowe, jądrowe i gazowe oraz zapewnienie zróżnicowanego dostępu do źródeł i dróg dostaw surowców energetycznych. Kluczowa jest liberalizacja rynków energii oraz tworzenie warunków dla realizacji inwestycji w sektorze energetycznym. Istotnym elementem polityki państwa będzie zapewnienie stabilności dostaw oraz integracja systemów energetycznych z państwami członkowskimi UE.

103. **Utrzymywanie rezerw strategicznych.** Sprawny i racjonalny system rezerw strategicznych zapewnia wsparcie realizacji zadań w zakresie bezpieczeństwa i obrony państwa, odtworzenia infrastruktury krytycznej, złagodzenia zakłóceń w ciągłości dostaw służących funkcjonowaniu gospodarki i zaspokojeniu podstawowych potrzeb obywateli, ratowania ich życia i zdrowia, a także wypełnienia zobowiązań międzynarodowych Polski. Najważniejszym zadaniem w tym zakresie jest opracowanie i przyjęcie przez Radę Ministrów *Rządowego Programu Rezerw Strategicznych* oraz zapewnienie mu finansowania na poziomie, który umożliwi realizację zaplanowanych działań. Równie istotne jest zapewnienie sprawnego funkcjonowania systemu zapasów interwencyjnych ropy naftowej i paliw, zabezpieczających zaopatrzenie Polski w sytuacjach kryzysowych oraz jego optymalizacja w zakresie zarządzania zapasami i efektywności kosztowej.

104. **Wzmacnianie bezpieczeństwa żywnościowego.** Niezbędne jest wdrożenie polityki rolnej, która zwiększy odporność produkcji rolnej na niekorzystne zjawiska i utrzymanie kontroli nad ważnymi dla bezpieczeństwa państwa działami gospodarki żywnościowej oraz zagwarantuje właściwy poziom samowystarczalności żywnościowej.

105. **Ochrona środowiska naturalnego.** Działania zwiększające bezpieczeństwo ekologiczne będą się koncentrowały na poprawie stanu środowiska, zachowaniu różnorodności biologicznej oraz adaptacji do zmian klimatu, w szczególności poprzez uwzględnienie konieczności zapewnienia odpowiedniego poziomu inwestycji w źródła niskoemisyjne. W ramach ochrony środowiska kontynuowane będą działania na rzecz poprawy czystości powietrza, wód, gleb oraz właściwej gospodarki odpadami. Adaptacja do zmieniających się uwarunkowań klimatycznych i hydrologicznych wymaga wdrożenia nowych rozwiązań systemowych, ukierunkowanych między innymi na minimalizowanie skutków klęsk żywiołowych i ekstremalnych zjawisk pogodowych. Szczególne znaczenie w tym kontekście ma realizacja działań przeciwpowodziowych oraz usprawnienie systemu zarządzania kryzysowego. Istotne jest też

prowadzenie kampanii edukacyjnych upowszechniających ochronę środowiska, zachowanie różnorodności biologicznej oraz adaptację do zmian klimatu. Gospodarka wodna musi stać się priorytetem w skali całej gospodarki kraju.

106. **Zapewnienie bezpieczeństwa kluczowych struktur przestrzennych gospodarki narodowej.** Priorytetem polskiej polityki przestrzennego zagospodarowania kraju jest ograniczenie nadmiernego, chaotycznego rozprzestrzeniania się miast określane jako suburbanizacja. Pożądane jest tworzenie podsystemów społeczno-gospodarczych o strukturach otwartych, dużej samowystarczalności i komplementarności. Istotne jest tworzenie warunków dla skutecznej realizacji działań obronnych oraz uwzględnianie potrzeb obronnych kraju (w tym lokalizacji obiektów wojskowych) w planach zagospodarowania przestrzennego oraz przy podejmowaniu decyzji przestrzennych.

107. **Badania naukowe i prace rozwojowe na rzecz bezpieczeństwa i obronności.** Strategiczne dla państwa kierunki są określane w *Krajowym Programie Badań*. Dotyczą one obszarów aktywności państwa o zasadniczym znaczeniu dla jego postępu cywilizacyjnego, rozwoju społecznego i gospodarczego oraz stanowią istotny element budowania potencjału bezpieczeństwa państwa. Zasadniczym celem badań naukowych i prac rozwojowych powinna być możliwość praktycznego zastosowania uzyskanych wyników, zwłaszcza dla rozwoju zdolności operacyjnych Sił Zbrojnych RP oraz służb i instytucji odpowiedzialnych za bezpieczeństwo państwa i obywateli. Należy dążyć do zacieśnienia współpracy i silniejszego powiązania między odbiorcą końcowym a przemysłem i sektorem badawczo-rozwojowym, w szczególności w zakresie wspólnego finansowania i komercjalizacji wyników badań nad technologiami podwójnego zastosowania. Istotne będzie zwiększanie zaangażowania polskich ośrodków w interdyscyplinarne projekty i programy międzynarodowe, co pozwoli na zdobycie nowej wiedzy i doświadczeń oraz wzmocnienie potencjału i konkurencyjności polskich podmiotów.

ROZDZIAŁ IV. KONCEPCJA PRZYGOTOWAŃ STRATEGICZNYCH. STRATEGIA PREPARACYJNA

108. Różnorodność wyzwań i nieprzewidywalność zagrożeń sprawia, że system bezpieczeństwa narodowego powinien być zdolny do wszechstronnej reakcji na pojawiające się problemy: od lokalnych i ograniczonych w skutkach do obejmujących całe państwo. Powinien być przekształcany tak, by monitorować i prognozować potencjalne zagrożenia, szybko i adekwatnie na nie reagować oraz rozwijać zdolności do usuwania skutków sytuacji kryzysowych.

109. Podstawowym założeniem koncepcji działań przygotowawczych jest właściwe połączenie w systemie bezpieczeństwa narodowego jego składników militarnych i niemilitarnych, wewnętrznych i zewnętrznych. Działania te koncentrować się będą na realizacji trzech priorytetów preparacyjnych: stosownej integracji podsystemu kierowania bezpieczeństwem narodowym; profesjonalizacji podsystemów operacyjnych (obronnego i ochronnych); powszechności przygotowań podsystemów wsparcia (społecznych i gospodarczych). Kluczowe zadania wiążą się z ustanowieniem podstaw prawnych i organizacyjnych zintegrowanego systemu bezpieczeństwa narodowego oraz wdrożeniem zasad i procedur polityczno-strategicznego kierowania bezpieczeństwem narodowym, jednolitych we wszystkich stanach bezpieczeństwa państwa.

4.1. Podsystem kierowania bezpieczeństwem narodowym

110. Działania zmierzające do integrowania kierowania bezpieczeństwem narodowym obejmują niezbędne zmiany na płaszczyźnie instytucjonalnej, infrastrukturalnej, proceduralnej i legislacyjnej.

111. **Zmiany instytucjonalne**. Konieczne jest instytucjonalne wzmocnienie Rady Ministrów w zakresie kierowania bezpieczeństwem narodowym poprzez powołanie organu pomocniczego, którego zadaniem byłoby w pierwszej kolejności usprawnienie koordynacji służb specjalnych

i nadzoru nad nimi. W przyszłości rozważyć można rozszerzenie zakresu kompetencji tego organu o inne obszary bezpieczeństwa narodowego lub powołanie odrębnego organu pomocniczego Rady Ministrów.

112. **Zmiany infrastrukturalne**. Pilną potrzebą jest poprawa infrastruktury wykorzystywanej na potrzeby kierowania bezpieczeństwem narodowym zarówno w zakresie modernizacji obiektów specjalnych, jak i wykorzystania nowoczesnych urządzeń technicznych o wysokim poziomie bezpieczeństwa informacyjnego i telekomunikacyjnego. Ponadto uporządkowania wymaga wykorzystanie systemów teleinformatycznych związanych z ostrzeganiem i alarmowaniem. Priorytetowym zadaniem jest wprowadzenie, na potrzeby najwyższych władz państwa, specjalnych środków transportu powietrznego, zapewniających ciągłość funkcjonowania, odporność i strategiczną mobilność systemu kierowania bezpieczeństwem narodowym.

113. **Zmiany proceduralne.** Konieczne jest doskonalenie procedur planowania, organizowania, koordynacji i nadzoru w sferze bezpieczeństwa, zapewniające spójność kierowania bezpieczeństwem narodowym z systemem zarządzania rozwojem kraju. Wynika to z nierozłączności i wzajemnej zależności rozwoju i bezpieczeństwa oraz potrzeby kompleksowego i zintegrowanego podejścia do bezpieczeństwa. Istotne też będzie zapewnienie spójności zarządzania kryzysowego z reagowaniem obronnym poprzez określenie wspólnych obszarów ujętych w planach zarządzania kryzysowego i planach operacyjnych wszystkich szczebli. Należy dążyć do wprowadzenia na wszystkich szczeblach administracji publicznej jednego dokumentu planistycznego obejmującego sprawy obronne, zarządzania kryzysowego i obrony cywilnej.

114. **Zmiany legislacyjne**. Wdrożenie nowych rozwiązań integrujących kierowanie bezpieczeństwem narodowym wymagać może zmian legislacyjnych, które precyzyjnie określałyby rolę władz i instytucji państwowych w systemie bezpieczeństwa narodowego, narzędzia jakimi one dysponują oraz zasady koordynacji działań.

4.2. Podsystem obronny

115. Celem przygotowania podsystemu obronnego jest utrzymanie i jakościowa transformacja potencjału bezpieczeństwa narodowego w dziedzinie obronnej, z uwzględnieniem pierwszoplanowej potrzeby posiadania zdolności niezbędnych do zapewnienia bezpośredniego bezpieczeństwa własnego narodu i obywateli oraz terytorium i struktur państwa. Przygotowanie potencjału obronnego obejmuje rozwój dyplomacji, Sił Zbrojnych RP, służb specjalnych działających w sferze obronnej oraz przemysłowego potencjału obronnego. Wpisuje się ono we wzmocnienie zdolności obronnych NATO oraz budowę takich zdolności Unii Europejskiej. Obszarem wiążącym podsystem obronny z pozostałymi podsystemami jest planowanie obronne.

116. **Dyplomacja.** Priorytetem transformacji polskiej dyplomacji jest kontynuacja modernizacji służby zagranicznej. Obejmować ona będzie optymalizację sieci polskich placówek zagranicznych oraz realizację projektów inwestycyjnych służących poprawie wizerunku i standardów ich funkcjonowania. Wprowadzona zostanie reforma szkolenia i doskonalenia kadr oraz upowszechnione będą nowoczesne techniki zarządzania w MSZ i placówkach zagranicznych. Kontynuowana będzie informatyzacja i rozbudowa infrastruktury teleinformatycznej służby zagranicznej.

117. **Siły Zbrojne RP**. Do najpilniejszych zadań przygotowawczych w obszarze obrony narodowej należy kontynuacja rozwoju zdolności operacyjnych Sił Zbrojnych RP, z uwzględnieniem wymaganego poziomu interoperacyjności w ramach NATO. Podstawą tego rozwoju jest pozyskiwanie nowoczesnego sprzętu wojskowego, jak również utrzymanie i rozwój systemu jego zabezpieczenia. Priorytetowe znaczenie ma stworzenie nowego jakościow o narodowego systemu obrony powietrznej, w tym przeciwrakietowej. Konieczna jest także dalsza rozbudowa systemów informacyjnych, tak aby Siły Zbrojne RP uzyskały między innymi zdolności prowadzenia rozpoznania obrazowego oraz zdolności sieciocentryczne. Zinformatyzowanie systemów walki i wsparcia, wraz ze zwiększeniem mobilności wojsk

lądowych, powinno wzmocnić kluczowe z punktu widzenia obrony państwa zdolności związane z działaniami przeciw zaskoczeniu. Rozwijanie zdolności Sił Zbrojnych RP do rozpoznania i precyzyjnego rażenia wyselekcjonowanych obiektów oraz przeciwdziałania szerokiemu spektrum zagrożeń asymetrycznych będzie jednym z elementów skutecznego odstraszania. Rozwojowi zdolności operacyjnych Sił Zbrojnych RP musi towarzyszyć podnoszenie poziomu wyszkolenia i umiejętności profesjonalnego wykorzystywania zaawansowanej techniki wojskowej, w tym narzędzi informatycznych. Konieczne będzie rozwijanie w Siłach Zbrojnych RP zdolności do działań w cyberprzestrzeni, w tym stworzenie mechanizmów cyberobrony i wzmocnienie dedykowanych jej jednostek. Istotne jest też rozwijanie narodowych zdolności w zakresie kryptologii i nabycie pełnych zdolności w dziedzinie wytwarzania narodowych rozwiązań kryptograficznych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych. Osiąganie kompetencji Sił Zbrojnych RP w zakresie kryptologii powinno wynikać z jednolitej polityki kryptologicznej i jest czynnikiem krytycznym w zapewnieniu bezpieczeństwa teleinformatycznego.

118. Istotne jest dokończenie reformy systemu kierowania i dowodzenia siłami zbrojnymi, konsolidującej działanie połączonych organów dowodzenia wokół podstawowych funkcji planowania, dowodzenia ogólnego i dowodzenia operacyjnego.

119. Reformy wymaga funkcjonowanie Narodowych Sił Rezerwowych, które powinny stać się formacjami zwartymi, umożliwiającymi realne wzmocnienie i uzupełnienie zdolności operacyjnych zarówno na potrzeby lokalnego reagowania w sytuacjach kryzysowych, jak i w warunkach ich użycia do działań w obronie kraju. Zmiana ta powinna być połączona z szerszą reformą przygotowania rezerw mobilizacyjnych oraz budową systemu powszechnego bezpieczeństwa terytorialnego.

120. Zmiany w systemie szkolnictwa wojskowego powinny zmierzać do jego konsolidacji oraz być zorientowane na poprawę efektywności szkolenia i prowadzenia badań naukowych na potrzeby bezpieczeństwa i obronności państwa, poprawę wydatkowania środków publicznych, a także wpisanie obszaru szkolenia i doskonalenia zawodowego szeregowych i podoficerów w krajowy system edukacji oparty na Polskiej Ramie Kwalifikacji. Istotne jest usprawnienie systemu wojskowej opieki medycznej, ukierunkowanej na odbudowę korpusu medycznego oraz modernizację polowej techniki medycznej.

121. **Służby specjalne**. Priorytetowo w rozwoju służb specjalnych należy traktować jakość kadr tych służb oraz wdrożenie najnowszych zinformatyzowanych technicznych systemów wywiadowczych i kontrwywiadowczych. Wojskowe służby specjalne powinny być silniej zintegrowane z resortem obrony narodowej.

122. **Przemysłowy potencjał obronny**. Konieczne jest wzmocnienie konkurencyjności i innowacyjności krajowego przemysłu obronnego oraz związanego z nim sektora naukowo-badawczego. Administracja rządowa powinna tworzyć warunki prawne, zachęty inwestycyjne oraz mechanizmy instytucjonalno-koordynacyjne dla rozwoju przemysłowego potencjału obronnego, w tym dla zwiększenia jego innowacyjności. Ze strony podmiotów przemysłu obronnego konieczne jest lepsze rozpoznanie potrzeb głównych użytkowników sprzętu wojskowego, dywersyfikacja i uatrakcyjnienie oferty rynkowej w zakresie nowoczesnych wyrobów, a także poszukiwanie możliwości racjonalizacji asortymentu i kosztów produkcji oraz rozwijanie współpracy z zagranicznymi partnerami. Działania obydwu stron muszą być ukierunkowane na osiągnięcie wysokiej jakości produkcji zgodnie z oczekiwaniami Sił Zbrojnych RP oraz na uzyskanie takiego stopnia konkurencyjności, który pozwoliłby na partnerską współpracę z firmami europejskimi i światowymi koncernami zbrojeniowymi.

123. Rozwój krajowego przemysłu obronnego musi się odbywać w równowadze ze zobowiązaniami międzynarodowymi Polski, w tym związanymi z budową europejskiego rynku obronnego. Państwo polskie będzie wspierało konkurencyjność, przejrzystość i efektywność europejskiej bazy technologiczno-przemysłowej sektora obronnego, chroniąc jednocześnie własny podstawowy interes bezpieczeństwa i korzystając w tym celu z wszystkich

dostępnych instrumentów prawnych i politycznych. Przesłankami dla potrzeby ochrony tego interesu są między innymi konieczność zapewnienia ciągłości działań państwa w warunkach nagłego lub realnego zagrożenia jego bezpieczeństwa, bezpieczeństwo informacji oraz bezpieczeństwo dostaw sprzętu wojskowego i zabezpieczenie możliwości jego operacyjnego użycia.

4.3. Podsystemy ochronne

124. Celem przygotowania podsystemów ochronnych jest dostosowany do strategii operacyjnej rozwój (organizacyjny, techniczny, szkoleniowy) służb, straży oraz wszelkich instytucji odpowiedzialnych za ochronę ludności, porządek publiczny i zarządzanie kryzysowe, a także zapewniających swobodę korzystania z praw i wolności obywatelskich.

125. **Wymiar sprawiedliwości**. Do najważniejszych zadań przygotowawczych należy kompleksowa reforma funkcjonalna wymiaru sprawiedliwości. Jej celem jest zwiększenie sprawności, jakości i efektywności funkcjonowania sądownictwa powszechnego. Przyspieszeniu postępowań sądowych, zwiększeniu ich przejrzystości oraz usprawnieniu wymiany informacji służy kontynuacja informatyzacji i cyfryzacji wymiaru sprawiedliwości. Konieczne są też zmiany w działaniu zawodów i modelu edukacji prawniczej oraz zapewnienie lepszego dostępu do informacji prawnej i usług prawniczych. W systemie penitencjarnym niezbędne jest maksymalne wykorzystanie możliwości, jakie dają środki probacyjne, w tym zwiększenie możliwości stosowania systemu dozoru elektronicznego.

126. **Służby specjalne**. Zadania przygotowawcze w obszarze służb specjalnych ukierunkowane będą na poprawę ich organizacji, wyposażenia oraz szkolenia. Konieczne jest skorygowanie systemu nadzoru nad nimi oraz zwiększenie ich zdolności do przygotowania zintegrowanego produktu informacyjnego. Należy również zmierzać do ustanowienia standardów związanych z czynnościami operacyjno-rozpoznawczymi poszczególnych służb specjalnych, a w związku z narastającym transsektorowym charakterem zagrożeń - budować platformy współdziałania służb i innych instytucji przeciwdziałających zagrożeniom o szczególnej wadze dla bezpieczeństwa państwa.

127. **Instytucje przeciwdziałania i zwalczania terroryzmu i ekstremizmu**. Konieczne jest dalsze wzmacnianie koordynacji działań instytucji państwowych uczestniczących w systemie ochrony antyterrorystycznej kraju. Szansą na zwiększenie ich spójności i skuteczności będzie przygotowanie rządowego dokumentu strategicznego (programu antyterrorystycznego), obejmującego istotne aspekty polityki antyterrorystycznej.

128. **Instytucje właściwe do spraw cyberbezpieczeństwa.** Do najważniejszych zadań przygotowawczych w obszarze cyberbezpieczeństwa należy wdrożenie i rozwijanie systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym. Konieczne jest określenie zasad prowadzenia aktywnej obrony oraz budowa narodowego systemu obrony cybernetycznej, w tym rozwijanie Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej, kompatybilnego z systemami państw sojuszniczych. Istotne jest stworzenie narodowego ośrodka koordynacji, wspierającego organizację współpracy pomiędzy poszczególnymi podmiotami realizującymi zadania w zakresie cyberbezpieczeństwa i wymianę informacji oraz promującego dobre praktyki w dziedzinie cyberbezpieczeństwa. Ważne jest nabycie pełnych kompetencji do rozpoznawania, zapobiegania i zwalczania cyberzagrożeń oraz zdolności do wytwarzania polskich rozwiązań technologicznych przeznaczonych do zapewnienia odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni. Zapewnione zostaną odpowiednie warunki tworzenia i działania partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa.

129. Początkiem procesu wzmacniania odporności systemu teleinformatycznego Rzeczypospolitej Polskiej powinno być stworzenie obszarów bezpieczeństwa wybranych systemów teleinformatycznych istotnych dla bezpieczeństwa państwa oraz odpowiednio zabezpieczonych dróg komunikacji między nimi. W dalszej kolejności zbudowana zostanie

jednolita platforma teleinformatyczna, umożliwiająca bezpieczne przetwarzanie i wymianę danych pomiędzy jednostkami administracji publicznej.

130. Istotne jest też zwiększanie świadomości użytkowników o zagrożeniach w cyberprzestrzeni poprzez intensyfikację działań edukacyjnych na wszystkich poziomach nauczania, a także w formie szkoleń i kampanii społecznych. Wskazane jest uruchomienie specjalnych kierunków studiów związanych z bezpieczeństwem funkcjonowania w cyberprzestrzeni oraz rozwijanie programów badawczych w tym obszarze.

131. **Instytucje ochrony informacji niejawnych**. Kluczowym zadaniem przygotowawczym w tej sferze jest zapewnienie rządowej niejawnej łączności stacjonarnej i mobilnej. Ważnym zadaniem jest też ciągłe dostosowywanie rozwiązań prawnych, proceduralnych, fizycznych i technicznych do pojawiających się zagrożeń dla przechowywania, przetwarzania i wymiany informacji niejawnych. W tym kontekście istotne znaczenie posiada pogłębianie współpracy w ramach NATO i UE. Podstawowe znaczenie dla ochrony systemów teleinformatycznych ma rozwój i implementacja narodowych rozwiązań z zakresu kryptografii.

132. **Instytucje ochrony infrastruktury krytycznej**. Ochrona kluczowej infrastruktury państwa wymaga uporządkowania przepisów w celu stworzenia jednej kategorii obiektów infrastruktury krytycznej. Wiązać się to będzie z potrzebą zmian zarówno w przepisach dotyczących obiektów podlegających obowiązkowej ochronie, jak i obiektów podlegających szczególnej ochronie. Spójne przepisy zagwarantują podniesienie odporności wszystkich elementów infrastruktury krytycznej, za co odpowiadać powinien powołany ustawowo organ do spraw ochrony infrastruktury krytycznej. Nowe przepisy powinny również stworzyć system realnych zachęt dla właścicieli infrastruktury krytycznej do inwestowania w bezpieczeństwo.

133. **Służby porządku publicznego**. Skuteczne przeciwdziałanie naruszeniom porządku publicznego wymaga wzmocnionej koordynacji różnych aspektów funkcjonowania podsystemu ochronnego oraz dalszej modernizacji służb i formacji odpowiadających za ten obszar funkcjonowania państwa. W zakresie zwalczania przestępczości zorganizowanej konieczne jest usprawnienie zinstytucjonalizowanej wymiany informacji między wszystkimi służbami i instytucjami zaangażowanymi w przeciwdziałanie tej formie przestępczości. Istotne jest ustawiczne podnoszenie bezpieczeństwa w ruchu drogowym. Niezbędne jest usprawnienie zabezpieczenia imprez masowych, a także kontynuacja wysiłków związanych z przeciwdziałaniem przestępczości gospodarczej i narkotykowej oraz handlowi ludźmi. Dla zapewnienia skutecznego działania konieczne jest zintegrowanie systemów łączności służb, w tym budowa ogólnokrajowego cyfrowego systemu łączności radiowej.

134. **Służby bezpieczeństwa powszechnego (ratownictwo i ochrona ludności).** Warunkiem skutecznego przygotowania państwa do realizacji zadań ratowniczych w celu ochrony życia, zdrowia, mienia i środowiska oraz pomocy humanitarnej (rozumianej jako działania mające na celu zapewnienie warunków niezbędnych do przetrwania, podejmowane w fazie reagowania przez służby i organizacje ratownicze) jest optymalne wykorzystanie istniejących zasobów, w szczególności Krajowego Systemu Ratowniczo-Gaśniczego, Państwowego Ratownictwa Medycznego (PRM), Systemu Powiadamiania Ratunkowego oraz potencjału stowarzyszeń (ochotnicze straże pożarne) i innych organizacji pozarządowych (społeczne organizacje ratownicze) oraz zapewnienie sprawnych mechanizmów ich doskonalenia i współdziałania. Ważnym zadaniem jest i będzie doskonalenie standardów w danym obszarze ratowniczym, z uwzględnieniem obszarów współpracy pomiędzy poszczególnymi służbami i podmiotami ratowniczymi oraz szczególnych wymagań organizacji systemu PRM, którego jednostki udzielają świadczeń osobom w stanie nagłego zagrożenia zdrowotnego. Powiązany z problematyką ochrony ludności obszar obrony cywilnej wymaga kompleksowej transformacji i dostosowania do obecnej sytuacji społeczno-gospodarczej, w tym zobowiązań międzynarodowych. Pilnym zadaniem jest kontynuacja budowy Systemu Powiadamiania Ratunkowego oraz systemów służb bezpośrednio wykonujących zadania ratownicze. Poprawa współdziałania wyżej wymienionych podmiotów wymaga również zapewnienia im zintegrowanego systemu łączności radiowej.

135. W ochronie zdrowia należy kontynuować doskonalenie struktur związanych z ratownictwem medycznym, podstawową opieką zdrowotną oraz specjalistyczną bazą leczniczą. Istotne jest też doskonalenie przygotowań organizacyjno-planistycznych, proceduralnych i materiałowych do funkcjonowania w sytuacjach zagrożeń i w czasie wojny.

136. **Służby graniczne**. Z uwagi na rosnące znaczenie transgranicznego wymiaru bezpieczeństwa doskonalony będzie zintegrowany system zarządzania granicą UE/Schengen. Zwiększenie skuteczności państwa w walce z nielegalną migracją wymaga zmian kompetencji uczestników tego systemu, a zwłaszcza wynikających z poszerzenia funkcji i zadań Straży Granicznej i przekształcenia jej w formację graniczno-migracyjną.

137. **Służby ochrony najważniejszych organów władzy i administracji publicznej**. Dbałość o bezpieczeństwo najważniejszych organów władzy państwowej wymaga sprawnej służby ochronnej i nowoczesnych środków transportu. Doprecyzować należy zasady i procedury dotyczące transportu i przemieszczania się osób zajmujących najważniejsze stanowiska w państwie, zwłaszcza w zakresie regulacji sposobu realizacji lotów o statusie HEAD. Określić należy także ośrodek koordynujący bezpieczeństwo transportu lotniczego VIP.

138. **Inne podsystemy ochronne**. Rosnący udział sektora prywatnego w zapewnianiu bezpieczeństwa oraz potencjał prywatnych instytucji ochrony jest szansą na wzmocnienie bezpieczeństwa obywateli oraz racjonalizację wydatków państwa. Warunkiem koniecznym dla dalszego rozwoju prywatnego sektora usług ochrony osób i mienia jest doskonalenie nadzoru i kontroli nad jego działalnością. Konieczne jest także określenie jego roli i opracowanie zasad współpracy w systemie bezpieczeństwa państwa, zwłaszcza w stanach nadzwyczajnych.

4.4. Podsystemy społeczne

139. Celem przygotowania podsystemów społecznych bezpieczeństwa narodowego jest zapewnienie ich efektywnego funkcjonowania w razie zagrożenia i wojny oraz doskonalenie zasad, procedur i zdolności realizacji zadań społecznego wsparcia operacyjnych podsystemów.

140. **System ochrony dziedzictwa narodowego.** Niezbędna jest modyfikacja systemu ochrony dóbr kultury przed zagrożeniami powszechnymi i wojennymi oraz doskonalenie spójnej polityki kulturalnej i historycznej państwa, uwzględniającej wymogi współczesnej ekonomii oraz zmiany zachodzące w obecnym świecie. Powinna ona również umożliwiać sprawowanie efektywnego mecenatu państwa, zapewniać wystarczający wzrost środków na ochronę dóbr kultury i dziedzictwa narodowego oraz określać ich rolę w rozwoju jednostek i narodu. Sprawą istotną jest także odpowiednia edukacja kulturalna oraz historyczna, obejmująca promowanie obszarów związanych między innymi z tradycją i dziedzictwem, uwzględniająca jednocześnie współczesne realia, takie jak kultura masowa, turystyka oraz środki komunikacji społecznej.

141. **Instytucje edukacji dla bezpieczeństwa**. Działania na rzecz podnoszenia kompetencji w obszarze bezpieczeństwa wymagają intensyfikacji i lepszego skoordynowania. Większy nacisk należy położyć na jakość kształcenia w obszarach istotnych dla bezpieczeństwa państwa i obywateli w powszechnym systemie edukacji i w szkolnictwie wyższym, a także na doskonalenie zawodowe żołnierzy, funkcjonariuszy, personelu cywilnego wojska i służb, pracowników administracji publicznej oraz nauczycieli przedmiotu edukacja dla bezpieczeństwa. Wymagać to będzie uporządkowania kwestii kształcenia na poziomie wyższym prowadzonego w szczególności przez uczelnie nadzorowane przez Ministra Obrony Narodowej i ministra właściwego do spraw wewnętrznych, między innymi poprzez tworzenie spójnych programów nauczania na potrzeby zintegrowanego bezpieczeństwa narodowego oraz reformę szkolnictwa wojskowego. W tym kontekście warto rozważyć, aby korzystając z istniejącego potencjału i zasobów, przekształcić jedną lub kilka z tych uczelni w jakościowo nową uczelnię publiczną kształcącą w zakresie zintegrowanego bezpieczeństwa narodowego, realizującą programy nauczania w wymiarze transsektorowym i ponadresortowym, co pozwoliłoby na uzyskanie odpowiadającej potrzebom państwa jakości nauczania.

142. **Media w systemie bezpieczeństwa narodowego.** Wskazane jest dalsze rozwijanie i pogłębianie współpracy przedstawicieli instytucji państwowych i mediów zaangażowanych w ochronę bezpieczeństwa narodowego. Konieczna będzie poprawa przygotowania służb prasowych instytucji państwowych i dziennikarzy zajmujących się problematyką bezpieczeństwa narodowego oraz większe ukierunkowanie misji mediów publicznych na tę tematykę.

143. **Przeciwdziałanie zagrożeniom demograficznym.** Istotnym priorytetem państwa polskiego będzie dalsze przeciwdziałanie niekorzystnym tendencjom demograficznym. Obejmować ono będzie wzmocnioną politykę rodzinną oraz spójną politykę migracyjną. W obszarze polityki rodzinnej należy kontynuować działania na rzecz godzenia życia zawodowego z życiem prywatnym, w tym rozwijać opiekę instytucjonalną nad dziećmi oraz alternatywne formy opieki nad osobami starszymi. Ponadto, w działaniach państwa należy uwzględniać wspieranie osób powracających i rozważających zamiar powrotu do Polski.

144. **Bezpieczeństwo socjalne**. Bezpieczeństwo socjalne osób i rodzin będzie zapewniane między innymi przez spójny system zabezpieczenia społecznego. Planuje się stworzenie całościowego i efektywnego systemu zasiłków oraz świadczeń społecznych, stymulującego ekonomiczne usamodzielnianie się i podejmowanie zatrudnienia na otwartym rynku pracy oraz takiego, w którym unika się ryzyka długotrwałego wykluczenia społecznego.

4.5. Podsystemy gospodarcze

145. Celem przygotowań podsystemów gospodarczych bezpieczeństwa narodowego jest opracowanie i wdrożenie odpowiednich strategii i programów zapewniania bezpiecznego funkcjonowania podmiotów gospodarczych państwa w czasie zagrożenia i wojny oraz realizacja zadań gospodarczego wsparcia operacyjnych podsystemów systemu bezpieczeństwa narodowego.

146. **Instytucje bezpieczeństwa finansowego**. W warunkach światowego kryzysu finansowego szczególnego znaczenia nabiera sprawność instytucji odpowiedzialnych za bezpieczeństwo finansowe Polski. Skuteczniejsze zapobieganie zagrożeniom z pogranicza przestępstw finansowych oraz zapobieganie wykorzystywania luk w przepisach prawnych wymaga wzmocnionej współpracy i koordynacji instytucji odpowiedzialnych za bezpieczeństwo finansowe państwa oraz odpowiednich służb ochrony państwa. Pożądana jest większa aktywność wymiaru sprawiedliwości wobec podmiotów zagrażających swoim działaniem inwestorom lub gospodarce. Istotne też jest realizowanie strategii wejścia Polski do strefy euro oraz jej ewentualne aktualizowanie, gdyż przyjęcie europejskiej wspólnej waluty może stworzyć skuteczną ochronę przed zawirowaniami walutowymi i pozwoli Polsce na pełny udział w unijnych procesach decyzyjnych.

147. **Podmioty bezpieczeństwa energetycznego**. Do priorytetów przygotowawczych określających kierunki rozwoju i doskonalenia bezpieczeństwa energetycznego Polski należy zaliczyć uruchomienie przemysłowego wydobycia gazu ziemnego ze złóż niekonwencjonalnych, w tym opracowanie technologii wydobywczej dostosowanej do specyfiki krajowych złóż tego surowca, rozbudowę sieci przesyłowych i magazynów do przesyłu dodatkowych ilości gazu ziemnego do odbiorców krajowych i zagranicznych oraz budowę regionalnego centrum dystrybucyjno-magazynowego gazu ziemnego na terytorium Polski. Należy rozbudować terminal LNG o kolejne możliwości regazyfikacyjne oraz istniejące i nowe połączenia gazowe w ramach Grupy Wyszehradzkiej w celu budowy regionalnego rynku gazu. Kontynuować należy prace na rzecz zróżnicowania źródeł dostaw ropy naftowej, w tym komercyjnej realizacji projektu dotyczącego importu surowca z rejonu Morza Kaspijskiego oraz wsparcie dla uruchomienia przemysłowego wydobycia ropy naftowej ze złóż niekonwencjonalnych w Polsce. Ważna jest także postępująca modernizacja systemu magazynowania, przesyłu i dystrybucji ropy naftowej i paliw w kraju oraz planowane polepszenie parametrów terminalu naftowego. Istotna jest przebudowa sektora wytwarzania energii elektrycznej, z uwzględnieniem priorytetu, jakim jest wykorzystanie krajowych złóż nośników energii pierwotnej (węgiel kamienny,

brunatny i gaz, w tym ze złóż niekonwencjonalnych) oraz energetyki jądrowej. W tym celu koniecznym jest zapewnienie wsparcia państwa dla długoterminowych, kapitałochłonnych inwestycji w nowe moce w elektroenergetyce. Bezpieczeństwo państwa wymaga międzyresortowej koordynacji, z uwzględnieniem podziału kompetencji w Radzie Ministrów w zakresie polityki energetycznej oraz zapewnienia wpływu państwa na jej realizację przez przedsiębiorstwa energetyczne, co umożliwi szybką i skuteczną reakcję w przypadku pojawienia się zagrożeń na rynkach energetycznych. Konieczne jest zachowanie przez państwo kontroli nad kluczową infrastrukturą sektora paliwowo-energetycznego oraz rozszerzenie nadzoru i kontroli nad bogactwem zasobów geologicznych państwa.

148. **System rezerw strategicznych**. Kluczowym zadaniem w zakresie utrzymania systemu rezerw strategicznych jest zapewnienie finansowania z budżetu państwa dla *Rządowego Programu Rezerw Strategicznych* na poziomie umożliwiającym realizację zadań zaplanowanych w perspektywie pięciu lat.

149. **Bezpieczeństwo żywnościowe**. W celu właściwej ochrony zdrowia i interesów konsumentów artykułów rolno-spożywczych istotne jest wzmocnienie kontroli żywności, tak aby działania państwowe zapewniały jednolity i sprawny nadzór nad jej produkcją i dystrybucją.

150. **Podmioty ochrony środowiska naturalnego**. Z uwagi na rozproszenie kontroli przestrzegania prawa dotyczącego ochrony środowiska w Polsce, podjęte zostaną prace nad wzmocnieniem i usprawnieniem działań służb ochrony środowiska. Rozwijana będzie współpraca międzynarodowa w obszarze bezpieczeństwa ekologicznego, wspierająca organizacje i porozumienia międzynarodowe na rzecz ograniczania emisji zanieczyszczeń, globalnej polityki klimatycznej i zachowania różnorodności biologicznej, respektujące poziom rozwoju i strukturę gospodarek narodowych państw uczestniczących.

151. **Jednostki naukowe.** Konieczne jest zwiększenie nowoczesności i innowacyjności potencjału naukowo-badawczego w obszarze bezpieczeństwa i obronności państwa poprzez aktywizację współpracy naukowo-przemysłowej (w tym międzynarodowej) środowiska naukowo-badawczego. Potrzeby zintegrowanego systemu bezpieczeństwa narodowego wymagają interdyscyplinarnego podejścia do badań naukowych i prac rozwojowych z zakresu bezpieczeństwa narodowego, między innymi poprzez wspólne finansowanie badań nad technologiami podwójnego zastosowania, możliwych do komercyjnego wykorzystania również w sektorze cywilnym. Kluczowe dla zwiększenia potencjału naukowego jest zapewnienie wieloletniej perspektywy stabilnego finansowania badań naukowych i prac rozwojowych w obszarach uznanych za priorytetowe ze względu na bezpieczeństwo narodowe. Należy dążyć do ustalenia proporcji nakładów na badania naukowe i prace rozwojowe z obszaru bezpieczeństwa i obronności państwa w relacji do wysokości PKB w poszczególnych latach budżetowych w drodze ustawowej. Zmierzać należy również do zwiększenia nakładów na badania i rozwój w dziedzinie bezpieczeństwa, w tym obronności, także poprzez poszukiwanie pozabudżetowych źródeł finansowania oraz szerokie wykorzystywanie dostępnych instrumentów (prawnych, finansowych, organizacyjnych), ułatwiających krajowym podmiotom prowadzenie działalności naukowo-badawczej.

ZAKOŃCZENIE

152. Za realizację postanowień niniejszej strategii odpowiadają ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, organy samorządu terytorialnego oraz inne podmioty, we właściwościach których pozostają sprawy z zakresu bezpieczeństwa państwa.

153. Treści *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* są rozwijane w *Polityczno-Strategicznej Dyrektywie Obronnej Rzeczypospolitej Polskiej* oraz *Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, realizującej długo- i średniookresową strategię rozwoju kraju.

154. Weryfikacja ustaleń zawartych w *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* oraz wypracowanie propozycji jej aktualizacji, odbywać się będzie między innymi w ramach Strategicznych Przeglądów Bezpieczeństwa Narodowego.

155. Niniejsza *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* zastępuje strategię zatwierdzoną przez Prezydenta Rzeczypospolitej Polskiej w dniu 13 listopada 2007 roku.

STRATEGICZNE PROBLEMY BEZPIECZEŃSTWA EUROPEJSKIEGO

W latach 2013-2014 z inicjatywy Biura Bezpieczeństwa Narodowego odbył się cykl warsztatów strategicznych z udziałem sekretarzy rad bezpieczeństwa narodowego państw Grupy Wyszehradzkiej – Polski, Czech, Słowacji oraz Węgier.

Ich celem było opracowanie wspólnego stanowiska dotyczącego wzmocnienia polityki bezpieczeństwa Unii Europejskiej, w tym nowelizacji Europejskiej Startegi Bezpieczeństwa z 2003 r.

Niniejsza synteza rezultatów warsztatów oraz konsultacji, została opublikowana za zgodą wszystkich stron w lipcu 2014 r.

BIURO BEZPIECZEŃSTWA NARODOWEGO

29 lipca 2014 r.

STRATEGICZNE PROBLEMY BEZPIECZEŃSTWA EUROPEJSKIEGO

Rada Europejska w grudniu 2013 r. zwróciła się do Wysokiego Przedstawiciela ds. Zewnętrznych i Polityki Bezpieczeństwa, aby „w ścisłej współpracy z Komisją ocenił wpływ zmian w środowisku globalnym oraz by, po konsultacjach z państwami członkowskimi, przedstawił Radzie w 2015 r. sprawozdanie dotyczące wyzwań i możliwości stojących przed Unią”.

Konkluzja ta zobowiązuje do refleksji nad strategicznymi problemami bezpieczeństwa UE. Jest ważne, aby uwzględniała ona kompleksowe podejście do bezpieczeństwa i obejmowała: misję UE w dziedzinie bezpieczeństwa, jej międzynarodowe otoczenie i warunki bezpieczeństwa, możliwe kierunki działań UE oraz niezbędny zakres przygotowań pozwalających skutecznie realizować tę misję.

Innymi słowy: proces ten powinien mieć w swej istocie charakter strategicznego przeglądu bezpieczeństwa europejskiego, a przygotowany w jego wyniku raport do debaty na Radzie Europejskiej w 2015 roku, być swego rodzaju Białą Księgą Bezpieczeństwa UE, zawierającą różne możliwe scenariusze i opcje działania.

Raport Wysokiego Przedstawiciela ds. Zewnętrznych i Polityki Bezpieczeństwa mógłby stać się podstawą do przygotowania nowej Europejskiej Strategii Bezpieczeństwa, jeżeli szczyt Rady Europejskiej w 2015 roku uzna taką potrzebę. Powinniśmy zmierzać w perspektywie do takiego właśnie celu. Dlatego ważne jest wcześniejsze merytoryczne przedyskutowanie i próba uzgodnienia między państwami UE strategicznych problemów bezpieczeństwa europejskiego. Uważamy, że takie podejście będzie stanowiło istotne wsparcie dla działań państw członkowskich w pracach nad raportem.

Niniejsze opracowanie powstało jako żywy dokument w wyniku wykorzystania rezultatów warsztatów strategicznych prowadzonych w 2013 roku w ramach Grupy Wyszehradzkiej na szczeblu doradców ds. bezpieczeństwa oraz sekretarzy rad bezpieczeństwa narodowego tych państw. Stanowi on punkt odniesienia do narodowych i międzynarodowych konsultacji. Kwestie bezpieczeństwa UE ujęte są w czterech blokach dotyczących:

1. Misji Unii Europejskiej w dziedzinie bezpieczeństwa,
2. Środowiska bezpieczeństwa,
3. Działań UE w dziedzinie bezpieczeństwa,
4. Środków niezbędnych do prowadzenia wspólnych działań.

1. MISJA UNII EUROPEJSKIEJ W DZIEDZINIE BEZPIECZEŃSTWA

Interesy narodowe i cele strategiczne są ważnymi punktami odniesienia podczas rozpatrywania problemów bezpieczeństwa. Można przyjąć, że uznane za wspólne interesy i cele strategiczne państw członkowskich stanowią misję UE w dziedzinie bezpieczeństwa i mogą być

rozpatrywane co najmniej w trzech wymiarach: 1) byt polityczny istniejący w określonej granicami przestrzeni (terytorium); 2) obywatele, jako swoiste atomy tej całości; 3) indywidualne i zbiorowe zasoby/dobra/wartości materialne (gospodarcze) i niematerialne (społeczne).

Mając na uwadze powyższe założenia misja UE w dziedzinie bezpieczeństwa mogłaby obejmować:

- wspieranie niepodległości i nienaruszalności granic państw członkowskich, głównie w wymiarze politycznym i gospodarczym oraz w innych pozamilitarnych dziedzinach i sektorach bezpieczeństwa, a jeśli państwa wzajemnie to uzgodnią – także w dziedzinie militarnej;
- współpraca na rzecz wzmacniania wspólnych i indywidualnych zdolności państw członkowskich do zapewniania bezpieczeństwa;
- działania na rzecz zapewnienia wolnego i bezpiecznego życia obywateli państw UE oraz swobody korzystania przez nich z praw i wolności człowieka i obywatela zarówno na terytorium UE, jak i poza nim, bez szkody dla bezpieczeństwa innych osób i bezpieczeństwa państw członkowskich;
- wspieranie ochrony indywidualnej obywateli i zbiorowej ludności przed zdarzeniami losowymi i zamierzonymi zagrożeniami dla ich życia i zdrowia oraz przed naruszeniem, utratą lub degradacją dysponowanych przez nich dóbr (materialnych i niematerialnych);
- wspólne działanie na rzecz bezpieczeństwa zrównoważonego rozwoju społeczno-gospodarczego państw UE;
- ukierunkowanie społecznego i gospodarczego działania na rzecz wsparcia rozwoju i umacniania systemu bezpieczeństwa UE.

2. ŚRODOWISKO BEZPIECZEŃSTWA

Analiza środowiska bezpieczeństwa UE prowadzona jest pod kątem zagrożeń, wyzwań i szans w perspektywie 10-15 lat w trzech wymiarach: globalnym, regionalnym (Afryka Północna, Bliski Wschód, Europa Wschodnia) oraz wewnętrznym (państwa członkowskie UE).

W wymiarze globalnym główne zagrożenia generowane będą przez dynamicznie narastające cyberzagrożenia, terroryzm międzynarodowy oraz proliferację broni masowego rażenia i środków jej przenoszenia, a także regionalne konflikty angażujące głównych graczy światowych. Źródłem głównych wyzwań będzie globalizacja oraz rewolucja informacyjna i biotechnologiczna. Za główną szansę zapewnienia bezpieczeństwa i rozwoju całej UE należałoby uznać możliwość pokojowego wykorzystania globalnych dóbr wspólnych (oceany, przestrzeń powietrzna, kosmiczna i cyber).

W wymiarze regionalnym główne zagrożenia będą stwarzane przez wewnątrzpaństwowe lub regionalne konflikty w bliskim sąsiedztwie UE (Europa Wschodnia, Bliski Wschód i Afryka Północna), państwa upadłe i upadające oraz ataki cybernetyczne. Główne wyzwania dla bezpieczeństwa europejskiego wiążą się ze sposobami radzenia sobie z konsekwencjami obecnego kryzysu bezpieczeństwa w Europie, a także z erozją nuklearnych i konwencjonalnych porozumień w zakresie kontroli zbrojeń, w tym traktatu o konwencjonalnych siłach zbrojnych w Europie (CFE). Największą szansę stwarzają demokratyczne przemiany ustrojowe oraz nowe rynki zbytu i inwestycyjne otwierające się w otoczeniu Europy.

W wymiarze wewnętrznym główne zagrożenie może powodować techniczna i technologiczna dekapitalizacja energetycznej infrastruktury krytycznej, cyberataki skierowane przeciwko systemom sterującym infrastrukturą krytyczną, formy terroryzmu charakterystyczne dla Europy (np. terroryzm separatystyczny, terroryzm rodzimy). Główne wyzwania będą wiązały

się z utrzymaniem spójności UE, jej finansową integracją oraz dywersyfikacją i pogłębieniem integracji na unijnym rynku energetycznym. Najważniejszą szansę dla wspólnoty europejskiej stwarza rozwój energetyki z wykorzystaniem zasobów gazu łupkowego oraz źródeł energii odnawialnej.

Biorąc pod uwagę prawdopodobieństwo wystąpienia wyżej wymienionych zjawisk i procesów oraz ich systemowy wpływ na bezpieczeństwo UE, można wyróżnić trzy scenariusze możliwego rozwoju strategicznych warunków (środowiska) bezpieczeństwa europejskiego:

- **realistyczny, najbardziej prawdopodobny (ewolucja)** - uwzględniający kontynuację obecnych trendów. Można zatem spodziewać się dalszego postępowania procesów integracyjnych w Europie (chociaż o znacznie zwolnionym tempie i zróżnicowanym charakterze) oraz utrzymania się, mimo kryzysów, podstawowych elementów spójności UE. Utrzymywać się będzie nadal ograniczona zdolność działania UE na arenie międzynarodowej, z jednoczesnym powolnym zmierzaniem w kierunku pogłębienia współpracy w dziedzinie bezpieczeństwa. Trudności mogą powodować działania rosyjskie nastawione na ograniczanie tej współpracy i rozbijanie jedności europejskiej;
- **bardzo korzystny, optymistyczny (zaawansowana integracja**) - uwzględniający przewagę
  pozytywnych oraz pożądanych zjawisk i tendencji w kształtowaniu się przyszłego środowiska. Może on zaistnieć, jeśli Europa powróci na ścieżkę wzrostu gospodarczego, pokona kryzys strefy euro, umocni się wspólna waluta; nastąpi pogłębienie integracji europejskiej w kierunku pełnej federacji z wspólną polityką bezpieczeństwa i obronną, bliską i efektywną współpracą z NATO; warunkiem takiego scenariusza jest kontynuowanie polityczno-wojskowej obecności USA na kontynencie europejskim oraz powrót Rosji na drogę współpracy z Zachodem;
- **wybitnie niekorzystny, pesymistyczny (dezintegracja)** – to scenariusz uwzględniający przewagę niekorzystnych i niebezpiecznych zjawisk zewnętrznych i wewnętrznych. Dla UE oznaczałoby to: pogłębiający się kryzys polityczny i finansowo-gospodarczy, prowadzący do osłabienia jej spójności; renacjonalizację polityk bezpieczeństwa państw członkowskich UE; spadek stopnia poszanowania prawa międzynarodowego, w tym wspólnotowego prowadzący do powstania „unii dwóch prędkości", a w dalszej perspektywie nawet do upadku waluty euro i dezintegracji UE. Jednym z ważnych elementów tego scenariusza byłyby konfrontacyjne działania Rosji (nowa zimna wojna).

3. DZIAŁANIA UE W DZIEDZINIE BEZPIECZEŃSTWA

Koncepcja działań strategicznych UE (tj. realizacji swojej uzgodnionej misji z uwzględnieniem przewidywanych warunków) powinna być dostosowana przede wszystkim do najbardziej prawdopodobnego scenariusza ewolucji, ale z uwzględnieniem także gotowości do koniecznych z punktu widzenia bezpieczeństwa korekt zwiększających wspólne wysiłki w razie wystąpienia scenariusza dezintegracji bądź też korekt dających możliwość przesunięcia wysiłków na zadania rozwojowe w razie scenariusza zaawansowanej integracji. W związku z tym za zasadne uznaje się rekomendowanie następujących strategicznych priorytetów działań UE w dziedzinie bezpieczeństwa:

- utrzymywanie i demonstrowanie jedności, determinacji i gotowości do działania w pełnym spectrum bezpieczeństwa;
- umacnianie międzynarodowej wspólnoty bezpieczeństwa, w szczególności poprzez działania na rzecz pogłębiania procesów integracyjnych opartych na wspólnocie interesów i wartości, w tym zwłaszcza rozwijanie WPBiO, wspólne europejskie

bezpieczeństwo energetyczne i cyberbezpieczeństwo, jak też współpracy z NATO oraz wzmacnianie strategicznych partnerstw, przede wszystkim z USA;

- wspieranie i uczestniczenie, na podstawie wyraźnego mandatu międzynarodowego, w działaniach społeczności międzynarodowej mających na celu zapobieganie powstawaniu źródeł zagrożeń lub rozprzestrzenianiu się już istniejących kryzysów.

Działania strategiczne UE w dziedzinie bezpieczeństwa mogą obejmować:

- stabilizowanie środowiska bezpieczeństwa - promowanie i rozwijanie współpracy wewnątrz i na zewnątrz UE, wykorzystywanie szans, podejmowanie wyzwań i zapobieganie zagrożeniom wwymiarze niemilitarnym, zwłaszcza energetycznym i cybernetycznym, a także militarnym;
- reagowanie kryzysowe - wzajemne wsparcie w zakresie monitorowania, informowania, przeciwdziałania kryzysom niemilitarnym, zwłaszcza energetycznym i cybernetycznym oraz spowodowanych klęskami i katastrofami, a także uzgodnione reagowanie na kryzysy poza terytorium UE, zagrażające interesom ujętym we wspólnej misji UE;
- działania obronne - wzajemne wspieranie się, zgodnie z Traktatem Lizbońskim, w zakresie odstraszania i odpierania agresji szczególnie w jej pozamilitarnych wymiarach (cyber, terror, inne).

4. ŚRODKI NIEZBĘDNE DO PROWADZENIA WSPÓLNYCH DZIAŁAŃ (system bezpieczeństwa UE)

Przygotowanie UE do działań w dziedzinie bezpieczeństwa powinno w pierwszej kolejności skupiać się na następujących priorytetach:

- koordynacji współpracy i współdziałania unijnych instytucji zarządzania bezpieczeństwem;
- profesjonalizacji podmiotów obronnych i ochronnych w państwach członkowskich, w tym sił zbrojnych, służb i straży, a w szczególności zbudowania systemu bezpieczeństwa energetycznego oraz profesjonalnego i powszechnego systemu cyberbezpieczeństwa;
- powszechniejszym zaangażowaniu w sprawy bezpieczeństwa podmiotów społecznych (w tym informacyjnych, kulturowych, edukacyjnych i naukowo-technicznych) i gospodarczych (w tym zwłaszcza przemysłowych, finansowych, energetycznych, infrastrukturalnych).
  Utrzymywanie i transformacja europejskiego systemu bezpieczeństwa wymaga następujących działań przygotowawczych:
- rozwój obecnych i ustanowienie nowych proceduralnych, instytucjonalnych, prawnych i doktrynalnych ram współpracy w ramach unijnego systemu zarządzania bezpieczeństwem, w tym stworzenie efektywnego systemu planowania strategicznego (strategie, plany rozwoju, programy, itp.);
- rozwój europejskich zdolności obronnych i w innych dziedzinach bezpieczeństwa, m. in. Poprzez strategicznie ukierunkowaną zrównoważoną konsolidację przemysłowego potencjału obronnego państw europejskich;
- umacnianie europejskiego obszaru wolności, bezpieczeństwa i sprawiedliwości;
- rozwój niematerialnych (w tym informacyjnych, edukacyjnych, kulturowych, naukowotechnicznych) i materialnych (finansowych, energetycznych, infrastrukturalnych) zdolności do wspierania działań na rzecz bezpieczeństwa europejskiego;

- rozwój zdolności niezbędnych do zapobiegania, ochrony, eliminowania i zwalczania zagrożeń oraz ryzyk związanych z cyberprzestępczością, terroryzmem i międzynarodową przestępczością zorganizowaną.

Konsultacje w różnych formatach regionalnych dotyczące strategicznych problemów bezpieczeństwa europejskiego mają szansę przyczynić się do kształtowania korzystnego klimatu politycznego podczas konsultowania Raportu Wysokiego Przedstawiciela przed Szczytem Rady Europejskiej w 2015 roku, jak również do stworzenia bazy wiedzy, która może okazać się przydatna do opracowania nowego dokumentu ramowego polityki bezpieczeństwa UE - Białej Księgi Bezpieczeństwa Europejskiego, a w dalszej perspektywie zapewne również Europejskiej Strategii Bezpieczeństwa.

UZASADNIENIE
DO PRZYGOTOWANEGO W BBN PROJEKTU USTAWY USPRAWNIAJĄCEJ KIEROWANIE OBRONĄ PAŃSTWA

10 lipca 2014 r. Prezydent RP Bronisław Komorowski przesłał do Sejmu RP przygotowany w BBN projekt ustawy o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw.

Celem ustawy było usprawnienie kierowania obroną państwa w czasie wojny i dostosowanie go do dynamicznie zmieniających się warunków bezpieczeństwa.

Przyjęta przez Parlament ustawa została podpisana przez Prezydenta RP 1 kwietnia 2015 r.

BIURO BEZPIECZEŃSTWA NARODOWEGO

10 lipca 2014 r.

UZASADNIENIE DO PRZYGOTOWANEGO W BBN PROJEKTU USTAWY O ZMIANIE USTAWY O POWSZECHNYM OBOWIĄZKU OBRONY RZECZYPOSPOLITEJ POLSKIEJ ORAZ NIEKTÓRYCH INNYCH USTAW, USPRAWNIAJĄCEJ KIEROWANIE OBRONĄ PAŃSTWA

Projektowana ustawa dotycząca zmiany *ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw*, ma na celu skorelowanie regulacji odnoszących się do funkcjonowania państwa w warunkach zagrożenia wojennego z przyjętą przez Sejm w dniu 21 czerwca 2013 r. zasadniczą reformą systemu kierowania i dowodzenia Siłami Zbrojnymi. Wychodzi ona jednocześnie naprzeciw złożonej przez Ministra Obrony Narodowej i Szefa Biura Bezpieczeństwa Narodowego, w toku prac parlamentarnych nad systemem kierowania i dowodzenia Siłami Zbrojnymi przy *ustawie o zmianie ustawy o urzędzie Ministra Obrony Narodowej oraz niektórych innych ustaw*, deklaracji przygotowania inicjatywy legislacyjnej, zmierzającej do dokonania w tym obszarze funkcjonowania państwa niezbędnych uzupełnień.

Pierwszą z projektowanych zmian jest propozycja określenia ram czasowych obowiązywania „czasu wojny" na terytorium Rzeczypospolitej Polskiej. W polskim prawodawstwie pojęcie „czas wojny" występuję w około 40 ustawach oraz w około 70 rozporządzeniach. Warto podkreślić, że ustawy te dotyczą wielu obszarów działalności państwa. Odnoszą się bowiem nie tylko do działalności organów administracji publicznej, ale również do przedsiębiorców i innych jednostek organizacyjnych, organizacji społecznych oraz osób fizycznych.

Jako przykład tego rodzaju regulacji należy wskazać przede wszystkim przepisy zawarte w art. 134 ust. 4 oraz w art. 175 ust. 2 Konstytucji RP, które warunkują konieczność mianowania Naczelnego Dowódcy Sił Zbrojnych oraz możliwość ustanowienia sądów wyjątkowych i trybu doraźnego od zaistnienia „czasu wojny", czy też przepisy ustawy o powszechnym obowiązku obrony RP przewidujące na „czas wojny" włączenie Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego w skład Sił Zbrojnych, jak również szczególne zasady pełnienia służby wojskowej i szczególny charakter świadczeń na rzecz obrony.

Regulacje dotyczącą „czasu wojny" budzą szereg wątpliwości interpretacyjnych, szczególnie w zakresie przedziału czasowego, w którym powinny one obowiązywać. Wpływa to w niekorzystny sposób na praktyczne ich stosowanie, co szczególnie uzewnętrzniło się podczas ćwiczeń dotyczących kierowania państwem w sytuacjach szczególnego zagrożenia.

Analiza prawna poruszonego problemu jednoznacznie wskazuje, że „czas wojny" nie jest tożsamy zarówno ze „stanem wojny" (art. 116 Konstytucji RP) jak i „stanem wojennym" (art. 229 Konstytucji RP).

„Czas wojny" to termin odnoszący się zasadniczo do czasu rzeczywistych działań wojennych (konfliktu zbrojnego na dużą skalę prowadzonego na terytorium naszego państwa). Jednocześnie jest to również pojęcie ustawowe warunkujące uruchomienie określonych reżimów prawnych, niezwykle istotnych z punktu widzenia bezpieczeństwa państwa, ale także wolności, praw i obowiązków obywateli. W praktyce może to rodzić szereg problemów decyzyjnych, gdyż trudno jednoznacznie stwierdzić, w którym dokładnie momencie mamy do czynienia z początkiem i końcem „czasu wojny".

W konsekwencji istnieje potrzeba precyzyjnego określenia, co w praktyce oznacza termin „czas wojny", bowiem ma to fundamentalne znaczenie w przypadku konieczności podwyższenia gotowości obronnej państwa i prowadzenia wojny oraz realizacji kompetencji poszczególnych jego organów, a także praw i obowiązków obywateli.

Biorąc za podstawę treść art. 126 ust. 2 Konstytucji, wyrażającą ustrojową funkcję Prezydenta RP jako strażnika suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium, w projekcie przewiduje się umocowanie Prezydenta RP do wydania postanowienia określającego dzień rozpoczęcia i dzień zakończenia „czasu wojny" (dodawany art. 4a ust. 1 pkt 4a w ustawie o powszechnym obowiązku obrony RP). Przewiduje się, że przesłanką wydania takiego postanowienia będzie zbrojna napaść na terytorium Rzeczypospolitej Polskiej. Należy podkreślić, że nie byłoby to autonomiczne uprawnienie Głowy Państwa, bowiem postanowienie w tej sprawie podlegałoby kontrasygnacie Prezesa Rady Ministrów, zgodnie z art. 144 ust. 2 Konstytucji RP.

Wprowadzenie tego przepisu pozwoli w sposób precyzyjny wskazać przedział czasowy, w którym do podwyższenia gotowości obronnej państwa oraz realizacji kompetencji poszczególnych organów, a także egzekwowania praw i obowiązków obywateli, będą stosowane przepisy mające obowiązywać w „czasie wojny".

W projekcie przewiduje się, że wyżej wymienione postanowienia Prezydenta RP podlegałyby niezwłocznemu ogłoszeniu w Dzienniku Ustaw Rzeczypospolitej Polskiej. Zgodnie bowiem z regulacjami zawartymi w *ustawie z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych*, w Dzienniku Ustaw ogłasza się akty prawne dotyczące w szczególności stanu wojny i zawarcia pokoju, powszechnej lub częściowej mobilizacji i użycia Sił Zbrojnych do obrony Rzeczypospolitej Polskiej (art. 9 ust. 2 ustawy). Postanowienie Prezydenta RP o dniu, w którym rozpoczyna się czas wojny na terytorium RP, a także postanowienie o dniu, w którym czas wojny się kończy – jako dotyczące tej samej materii – powinno być ogłaszane również w Dzienniku Ustaw. Należy dodać, że na zawarcie takiej regulacji w *ustawie o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* zezwala art. 9 ust. 3 wskazanej wyżej *ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych*, zgodnie z którym w Dzienniku Ustaw ogłasza się także inne akty prawne, jeżeli odrębne ustawy tak stanowią.

W projekcie proponuje się uzupełnienie treści art. 5 *ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* określającego sposób sprawowania przez Prezydenta RP zwierzchnictwa nad Siłami Zbrojnymi o kompetencje w zakresie zatwierdzania, na wniosek Ministra Obrony Narodowej, w drodze postanowienia, narodowych planów użycia Sił Zbrojnych do obrony państwa oraz organizacji i zasad funkcjonowania wojennego systemu dowodzenia Siłami Zbrojnymi. Są to podstawy rozstrzygnięć przygotowywanych już w czasie pokoju, a warunkujących realizację kompetencji Prezydenta RP w zakresie kierowania obroną państwa. Skoro bowiem organ ten posiada takie uprawnienia to w konsekwencji powinien mieć wpływ na treść najważniejszych dokumentów dotyczących obrony państwa i użycia Sił Zbrojnych.

Projekt zawiera także propozycję dookreślenia (poprzez dodanie art. 5a w *ustawie o powszechnym obowiązku obrony RP*) prawnej pozycji osoby wskazanej przez Prezydenta RP (na wniosek Prezesa Rady Ministrów) przewidzianej do mianowania na stanowisko Naczelnego Dowódcy Sił Zbrojnych. Zakłada się, że osoba ta będzie przygotowywana do realizacji zadań wynikających z kompetencji Naczelnego Dowódcy Sił Zbrojnych. Jednocześnie – wychodząc

naprzeciw postulatom zgłaszanym podczas prac parlamentarnych nad ustawą reformującą system kierowania i dowodzenia w Siłach Zbrojnych - proponuje się, aby osoba ta wykonywała czynności związane z przygotowywaniem się do pełnienia funkcji Naczelnego Dowódcy do czasu mianowania Naczelnego Dowódcy Sił Zbrojnych (niezależnie, czy na tego Dowódcę zostanie mianowana ta czy też inna osoba) albo wskazania (w takim samym trybie) innej osoby przewidzianej do mianowania na stanowisko Naczelnego Dowódcy Sił Zbrojnych. Zakłada się, że przygotowania te powinny obejmować problematykę dotyczącą w szczególności planowania, organizowania i przygotowaniu wojsk oraz systemów dowodzenia Siłami Zbrojnymi na potrzeby prowadzenia działań związanych z obroną państwa.

Ponadto proponuje się, aby Rada Ministrów, w drodze rozporządzenia, określiła właściwe podmioty i ich zadania w zakresie przygotowania osoby wskazanej do mianowania na Naczelnego Dowódcę Sił Zbrojnych do objęcia tego stanowiska, a także sposób jej udziału w tych przygotowaniach. W celu właściwego przebiegu tego procesu rozporządzenie powinno w szczególności zapewnić możliwość jej udziału w strategicznych grach i ćwiczeniach obronnych, planowaniu użycia Sił Zbrojnych do obrony państwa oraz w przygotowaniu wojennego systemu dowodzenia Siłami Zbrojnymi.

W procesie przygotowań powinny uczestniczyć różne podmioty, np. właściwe w sprawach przygotowania transportu, łączności, zdrowia, stanowisk kierowania na potrzeby obronne państwa (określeni ministrowie i kierownicy organów centralnych). W projekcie uwzględniono także udział Szefa Biura Bezpieczeństwa Narodowego w procesie przygotowania osoby wskazanej do mianowania na Naczelnego Dowódcę Sił Zbrojnych w zakresie uprawnień Prezydenta Rzeczypospolitej Polskiej dotyczących Naczelnego Dowódcy Sił Zbrojnych. Zadaniem wspomnianych podmiotów powinno być w szczególności zapoznanie osoby, o której mowa wyżej, z odpowiednimi dokumentami i procedurami odnoszącymi się do problematyki związanej z obroną państwa oraz zapewnienie jej udziału w przedsięwzięciach realizowanych przez Siły Zbrojne w mach tych potrzeb.

Przewiduje się również doprecyzowanie art. 11b ust. 2 pkt 1, określającego zakres działania Dowódcy Operacyjnego Rodzajów Sił Zbrojnych poprzez wskazanie, że planowanie, organizowanie i prowadzenie operacji w ramach użycia Sił Zbrojnych będzie realizowane przez ten organ jedynie do czasu mianowania Naczelnego Dowódcy Sił Zbrojnych.

Kolejne zmiany w *ustawie o powszechnym obowiązku obrony RP* są konsekwencją proponowanego określenia obowiązywania „czasu wojny" i zmierzają do ujednolicenia stosowanych w tym zakresie pojęć (art. 109a ust. 4 i 6 oraz art. 110).

Proponuje się również uchylenie w tej ustawie art. 247 ust. 1, stanowiącego, że „w czasie obowiązywania stanu wojennego stosuje się w zakresie obowiązku służby wojskowej, służby w obronie cywilnej i służby w jednostkach zmilitaryzowanych oraz świadczeń na rzecz obrony przepisy obowiązujące w czasie wojny, jeżeli Prezydent wprowadzając stan wojenny nie postanowi inaczej". Przepis ten w sposób sztuczny zrównuje pojęcia czasu wojny i stanu wojennego tylko dla części przepisów przygotowanych do obowiązywania w czasie wojny.

W sytuacji, kiedy Prezydent RP w czasie stanu wojennego, w razie zbrojnej napaści na terytorium RP, określi (zgodnie z dodawanym art. 4a ust. 1 pkt 4a) początek czasu wojny, od tego dnia będą obowiązywać przepisy odnoszące się do czasu wojny. W konsekwencji nie ma potrzeby, aby obowiązywała regulacja zawarta w art. 247 ust. 1. Innym argumentem przemawiającym za rezygnacją z tego przepisu jest okoliczność, że stan wojenny może zostać wprowadzony w przypadku udzielenia przez Polskę pomocy w ramach sojuszu wojskowego. Wówczas z mocy prawa powinny obowiązywać przepisy odnoszące się do czasu wojny (chyba że Prezydent RP postanowi inaczej). Tymczasem brak jest uzasadnienia dla takiej regulacji, bowiem przepisy te powinny obowiązywać dopiero od dnia, w którym rozpoczyna się czas wojny, którego początek (zgodnie z projektem) uzależniony będzie od zbrojnej napaści na polskie terytorium.

W projekcie proponuje się także dokonanie zmiany ustaw: o *Policji*, *o Straży Granicznej* i o *Służbie Więziennej*, które mają na celu zastąpienie terminu „wybuch wojny" pojęciem „czas wojny", a którego dzień rozpoczęcia i zakończenia będzie określał Prezydent Rzeczypospolitej Polskiej (na podstawie dodawanego art. 4a ust. 1 pkt 4a *ustawy o powszechnym obowiązku obrony RP*).

Następne zmiany dotyczą *ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*. Pierwsza z nich polega na umożliwieniu Prezydentowi RP korzystania z pomocy kompetentnego organu, który będzie mu doradzał w procesie kierowania obroną państwa. W projekcie przewiduje się, że organem tym będzie Szef Sztabu Generalnego Wojska Polskiego.

Niezależnie od powyższego proponuje się doprecyzowanie przepisu odnoszącego się do Sił Zbrojnych pozostających w podporządkowaniu Naczelnego Dowódcy Sił Zbrojnych (art. 16 ust. 2). Na tle obowiązującego brzmienia tego przepisu, od czasu uchwalenia ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej podnoszono wątpliwość, czy Naczelny Dowódca Sił Zbrojnych dowodzi całymi Siłami Zbrojnymi, czy tylko ich częścią. W projekcie wskazuje się, że organ ten będzie dowodził tymi Siłami Zbrojnymi oraz innymi jednostkami organizacyjnymi, które zostaną mu podporządkowane decyzją Ministra Obrony Narodowej, na potrzeby związane z obroną państwa. Celem tej regulacji jest doprecyzowanie zakresu dowodzenia sprawowanego przez Naczelnego Dowódcę Sił Zbrojnych, które powinno być zależne od strategicznych potrzeb obrony państwa, a jednocześnie mieścić się w zakresie kompetencji Prezydenta RP związanych z kierowaniem obroną państwa. Zadaniem Naczelnego Dowódcy Sił Zbrojnych podporządkowanego bezpośrednio Prezydentowi RP jest bowiem prowadzenie operacji obronnej w celu odparcia zbrojnej napaści wyłącznie na terytorium Rzeczypospolitej Polskiej. W podporządkowaniu tego Dowódcy powinny zatem pozostawać jedynie te wojska oraz jednostki organizacyjne, które są niezbędne do prowadzenia działań o takim charakterze.

Pozostałe zadania realizowane przez Siły Zbrojne będą w dalszym ciągu we właściwości Ministra Obrony Narodowej.

W toku prac nad opracowaniem niniejszego projektu ustawy przeprowadzono konsultacje m.in. z Ministerstwem Obrony Narodowej, przedstawicielami sejmowej i senackiej komisji obrony narodowej oraz klubów parlamentarnych. Główne założenia projektu zostały omówione z ekspertami z zakresu obronności i funkcjonowania sił zbrojnych.

Wejście w życie projektowanej ustawy nie pociąga za sobą skutków finansowych dla budżetu państwa.

Projekt ustawy nie jest objęty zakresem prawa Unii Europejskiej.

KONCEPCJA STRATEGICZNEJ ODPORNOŚCI KRAJU NA AGRESJĘ

Prace nad koncepcją strategicznej odporności kraju na agresję Biuro Bezpieczeństwa Narodowego podjęło na polecenie Prezydenta RP Bronisława Komorowskiego. Opracowanie oraz realizacja poszczególnych elementów koncepcji był odpowiedzią m.in. na zwiększone zagrożenie w regionie związane z agresją Rosji na Ukrainę.

Wzmocnienie i zintegrowanie systemu strategicznej odporności kraju jest także jedną z rekomendacji ze Strategicznego Przeglądu Bezpieczeństwa Narodowego.

Szef BBN przedstawił założenia koncepcji 30 kwietnia 2014 r. na spotkaniu z udziałem przedstawicieli m.in. Ministerstwa Obrony Narodowej, Ministerstwa Spraw Wewnętrznych, Sił Zbrojnych i poszczególnych niemilitarnych służb mundurowych.

BIURO BEZPIECZEŃSTWA NARODOWEGO

30 kwietnia 2014 r.

GENERALNY OPIS KONCEPCJI STRATEGICZNEJ ODPORNOŚCI KRAJU NA AGRESJĘ

Ideą systemu jest skoordynowanie różnych działań (legislacyjnych, operacyjnych, szkoleniowych, organizacyjnych, technicznych itp.) w wielu sektorach bepzpieczeństwa mające służyć zwiększeniu strategicznej odporności kraju na zagrożenia, jako jednemu z ważnych wymiarów współczesnego odstraszania (powstrzymywania, odstręczania), w tym także przed próbami "miękkiej", asymetrycznej agresji. Należą do nich przede wszystkim:

- Działania nieregularne na terytorium zajętym przez przeciwnika
- Militarne 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

Stosownie do tych działań powinny zostać określone zadania dla poszczególnych podmiotów. Takich jak wojska specjalne, zreformowane Narodowe Siły Rezerwowe, niewojskowe formacje bezpieczeństwa i ochrony ludności czy pozarządowe organizacje proobronne. To także zadania związane z doskonaleniem systemu rezerw mobilizacyjnych.

Prowadzenie oraz organizowanie działań nieregularnych na terytorium zajętym przez przeciwnika powinno być realizowane przez **Wojska Specjalne** W związku z tym rozważyć należy ukierunkowanie ich zadaniowo na obronę kraju (co powinno zostać ujęte m.in. w takich dokumentach jak Polityczno-Strategiczna Dyrektywa Obronna); zwiększenie ich liczebności (m.in. poprzez włączenie w ich skład Oddziałów Specjalnych Żandarmerii Wojskowej); oraz organizowanie szkolenia ich na terytorium kraju z pozostałymi strukturami państwa.

Zadaniem **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 operacyjne podporządkowanie Wojewódzkich Sztabów Wojskowych („wojsko wojewodów"), oraz aby w ich skład wchodzili przede wszystkim rezerwiści, a nie jak obecnie kandydaci do służby zawodowej.

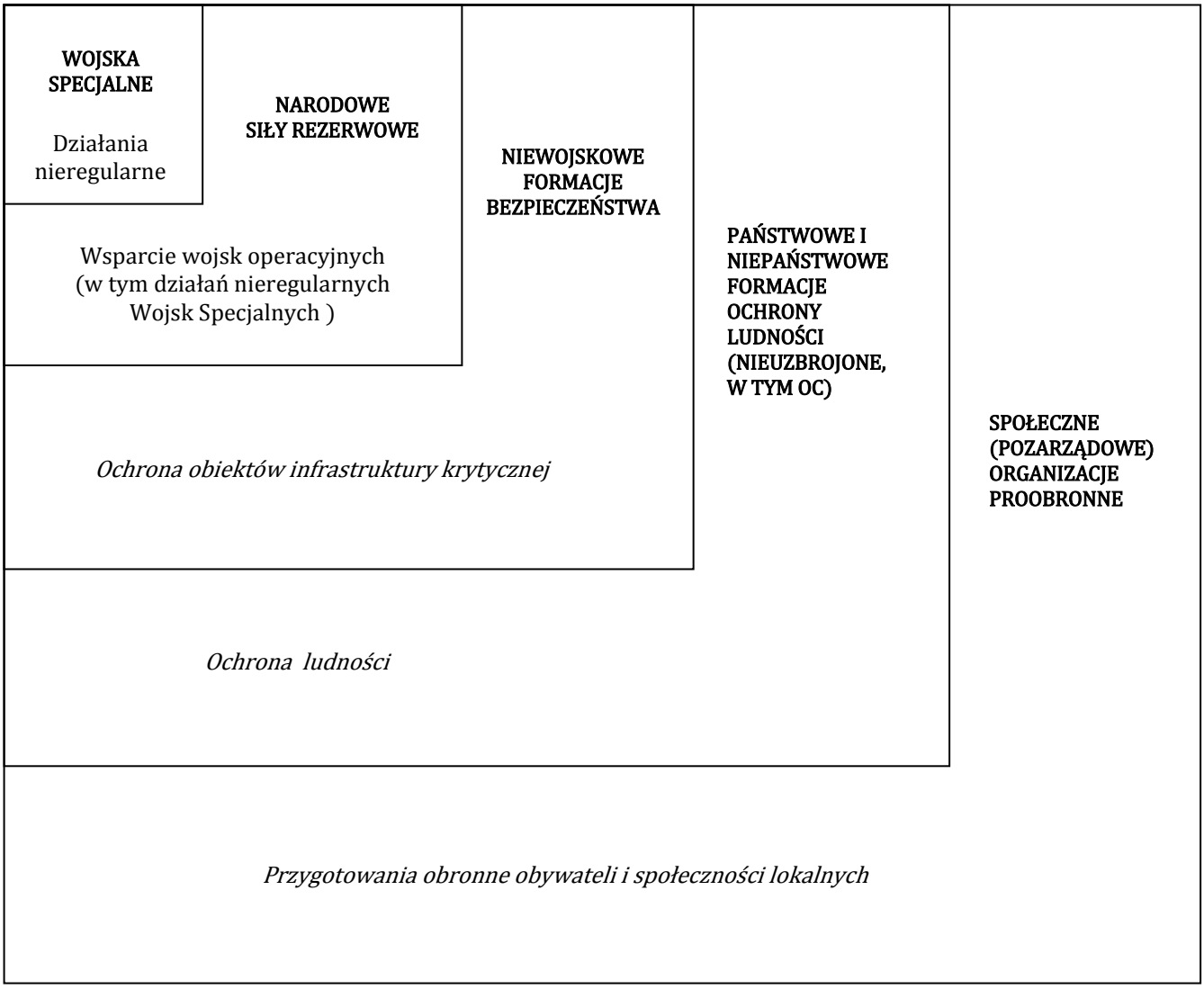
Konieczne jest **przygotowanie systemu rezerw mobilizacyjnych**, umożliwiających strategiczne rozwinięcie sił zbrojnych do wielkości i struktury czasu wojny oraz ich uzupełnianie w toku

działań wojennych. Do zadań w tym zakresie należałoby odpowiednie zaplanowanie potrzeb mobilizacyjnych, zorganizowanie zasobów mobilizacyjnych oraz szkolenie rezerw mobilizacyjnych.

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

Za ochroną ludności cywilnej przed skutkami zagrożeń militarnych i niemilitarnych w czasie wojny powinny odpowiadać określone **formacje ochrony ludności**. Zadania preparacyjne na tym obszarze powinny polegać m.in. na stworzeniu systemu ratowniczego z udziałem takich służb jak Państwowa Straż Pożarna czy pogotownia ratunkowe, wykorzystanie w systemie ratownictwa Ochotniczych Straży Pożarnych oraz stworzenie struktur Obrony Cywilnej na czas wojny.

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



"DOKTRYNA KOMOROWSKIEGO"

Termin odnosi się do nowej strategii w myśleniu o polskim bezpieczeństwie, którą można wiązać z działaniami Prezydenta RP Bronisława Komorowskiego. Jej kwintesencją było przenoszenie strategicznych priorytetów z zadań i działań ekspedycyjnych, na zapewnienie bezpieczeństwa terytorium państwa.

Główne założenia doktryny zostały przedstawione przez szefa BBN 15 kwietnia 2013 r.

BIURO BEZPIECZEŃSTWA NARODOWEGO

15 kwietnia 2013 r.

"DOKTRYNA KOMOROWSKIEGO"

"Doktryna Komorowskiego" to nieformalne określenie głównej myśli polityki realizowanej przez prezydenta Bronisława Komorowskiego odnoszącej się do strategii bezpieczeństwa państwa (w tym zwłaszcza do zadań sił zbrojnych) i wyrażającej się w przeniesieniu priorytetów z zaangażowania zewnętrznego na zadania związane z bezpośrednim bezpieczeństwem (obroną) kraju (narodu, terytorium, zasobów).

Doktryna bazuje na doświadczeniach i rekomendacjach z przeprowadzonego na polecenie Prezydenta w latach 2010-2012 Strategicznego Przeglądu Bezpieczeństwa Narodowego (szeroko zakrojonego audytu bezpieczeństwa państwa). Jej tezy zawarte zostały w opublikowanej w 2013 r. Białej Księdze Bezpieczeństwa Narodowego RP. Doktryna znalazła swoje dyrektywne odbicie m.in. w zatwierdzonej przez Prezydenta RP Strategii Bezpieczeństwa Narodowego RP.

1. Należy przenieść strategiczne priorytety Rzeczypospolitej Polskiej z udziału w misjach ekspedycyjnych na zadania związane z zapewnianiem bezpośredniego bezpieczeństwa, w tym obrony, państwa.

Znaczące zewnętrzne militarne zaangażowanie Polski w czasie ostatniej dekady (którego symbolem jest operacja w Afganistanie) oraz rozwijanie pod tym kątem potencjału wojskowego siłą rzeczy ograniczały możliwości optymalnego przygotowywania sił zbrojnych do realizacji ich najważniejszego, konstytucyjnego zadania, jakim jest bezpośrednie bezpieczeństwo, w tym zwłaszcza obrona państwa (narodu jako całości, obywateli, terytorium i zasobów). Dlatego też w interesie Polski leży, aby dokonać zwrotu w myśleniu o priorytetach dla sił zbrojnych i przekierować je na zadania obronne. Co należy zaznaczyć, doktryna nie zakłada rezygnacji z udziału w misjach zagranicznych. Postuluje jedynie nadanie udziałowi w nich właściwego miejsca w hierarchii zadań dla państwa i sił zbrojnych.

2. Własny potencjał obronny stanowi podstawowy filar oraz gwarancję naszego bezpieczeństwa.

Udział w sojuszach, zwłaszcza w NATO, to ważne zewnętrzne filary wspierające nasze bezpieczeństwo. Ale najważniejszym filarem są własne zdolności obronne. Dlatego konieczne jest utrzymanie stabilnych nakładów na siły zbrojne, które powinny być optymalnie wydawane na wzmacnianie w pierwszej kolejności zdolności potrzebnych do obrony własnego państwa (narodu, terytorium i zasobów) lub obrony terytorium sojuszników z NATO. Takie właśnie, obronne, zdolności powinny być naszą narodową specjalnością w NATO i je powinniśmy przede wszystkim wnosić do wspólnego potencjału sojuszniczego. Równolegle rozwijane powinny być także pozamilitarne zdolności państwa (instytucji publicznych, podmiotów prywatnych, obywateli) do funkcjonowania w warunkach zagrożenia tak, aby budować zintegrowany (połączony) system bezpieczeństwa narodowego.

3. Polską specjalizacją w NATO i UE powinny być także, obok zdolności do obrony terytorium, zdolności „przeciwzaskoczeniowe", konieczne zwłaszcza w sytuacjach trudnokonsensusowych.

Polska, jako państwo graniczne NATO i UE jest szczególnie narażona na zagrożenia o charakterze nagłym, niespodziewanym, selektywnym, na ograniczoną skalę – czyli takie, które nie wymagają dłuższych i zauważalnych zawczasu przygotowań, a jednocześnie mogą być skutecznym środkiem szantażu i wywierania presji polityczno-strategicznej. Takie zagrożenia niekoniecznie wiązać się muszą z zamiarem opanowania terytorium RP, a jedynie zadania strat (tzw. zagrożenia „aterytorialne"). Z tego względu stwarzają one sytuacje trudnokonsensusowe, czyli takie, w których sojusznicy mogliby mieć kłopoty w terminowym uzyskaniu konsensusu, co do celu, charakteru i skali reakcji. W związku z tym sojusz, jako całość, mógłby nie być w stanie szybko i skutecznie zareagować. Dlatego Polska powinna posiadać pełne spektrum narodowych zdolności do przeciwstawiania się właśnie tego typu zagrożeniom (głównie takie zdolności jak: wywiad i rozpoznanie, obrona powietrzna, w tym przeciwrakietowa, mobilność wojsk, zwłaszcza śmigłowcowa).

4. Polska powinna umacniać swoją podmiotowość strategiczną na arenie międzynarodowej, aktywnie uczestnicząc w funkcjonowaniu organizacji międzynarodowych i ich kształtowaniu stosownie do własnych interesów strategicznych.

W odniesieniu do NATO w polskim interesie jest, aby po zakończeniu operacji w Afganistanie sojusz konsolidował się wokół realizacji swojego podstawowego zadania, związanego z zapewnieniem bezpośredniego bezpieczeństwa państw członkowskich. W wymiarze praktycznym powinno to wyrażać się zwłaszcza w ciągłej aktualizacji planów ewentualnościowych (planów działania na wypadek agresji na członka NATO) oraz regularnym weryfikowaniu tych planów podczas sojuszniczych ćwiczeń wojskowych, a także proporcjonalnym rozwoju infrastruktury obronnej. Co do UE to nasze działania powinny zmierzać do wzmacniania Wspólnej Polityki Bezpieczeństwa i Obrony, aby mogła być drugim, obok NATO, zewnętrznym filarem wzmocnienia bezpieczeństwa Polski. Szczególnie ważne jest zwłaszcza przyjęcie realnej strategii bezpieczeństwa europejskiego, jako niezbędnego fundamentu dla upodmiotowienia UE w tej dziedzinie. Priorytetem dla Polski są też relacje euroatlantyckie, w tym systemowe współdziałanie NATO-UE.

UZASADNIENIE
DO PROJEKTU USTAWY REFORMUJĄCEJ SYSTEM KIEROWANIA I DOWODZENIA SIŁAMI ZBROJNYMI RP

12 marca 2013 r. rząd przyjął projekt ustawy o zmianie ustawy o urzędzie Ministra Obrony Narodowej oraz niektórych innych ustaw, przedłożony przez ministra obrony narodowej. Celem ustawy było usprawnienie systemu kierowania i dowodzenia Siłami Zbrojnymi.

Projekt zmian przygotowany został przy ścisłej współpracy Ministerstwa Obrony Narodowej oraz Biura Bezpieczeństwa Narodowego.

Ustawa podpisana została przez Prezydenta RP 22 lipca 2013 r.

12 marca 2013 r.

UZASADNIENIE
DO PROJEKTU O ZMIANIE USTAWY O URZĘDZIE MINISTRA OBRONY NARODOWEJ ORAZ NIEKTÓRYCH INNYCH USTAW REFORMUJĄCEJ SYSTEM KIEROWANIA I DOWODZENIA SIŁAMI ZBROJNYMI

Projekt ustawy jest wynikiem analizy, która wykazała, że podstawową słabością obecnego systemu jest skupienie w rękach jednego organu – Szefa Sztabu Generalnego Wojska Polskiego (z podległym mu Sztabem Generalnym WP) – różnych funkcji centralnego kierowania Siłami Zbrojnymi. Tymi funkcjami są: perspektywiczne, wieloletnie planowanie i programowanie strategiczne, dowodzenie ogólne oraz dowodzenie operacyjne Siłami Zbrojnymi. Za zasadnością opracowania projektu przemawia także potrzeba pełnego wdrożenia nowoczesnej idei „połączenia" (joint) do systemu kierowania i dowodzenia Siłami Zbrojnymi. Obecnie tylko jeden organ dowodzenia, a mianowicie Dowództwo Operacyjne, ma charakter dowództwa połączonego. Kolejną przesłanką projektowanej reformy jest rozdzielenie funkcji planowania, dowodzenia ogólnego i dowodzenia operacyjnego.

Zmiany proponowane w projekcie zmierzają do uproszczenia struktury kierowania i dowodzenia Siłami Zbrojnymi, a także wyraźnego rozdzielenia spraw polityczno-strategicznych i administracyjnych (wchodzących w zakres działania Ministra Obrony Narodowej) od spraw ogólnego dowodzenia Siłami Zbrojnymi i dowodzenia operacyjnego. Szczególnie istotne jest to, że zmiany te mają zapewnić także odpowiednie warunki organizacyjne do przygotowania dowództw do wojennego systemu dowodzenia Siłami Zbrojnymi, z uwzględnieniem potrzeb dowodzenia w układzie narodowym, sojuszniczym i koalicyjnym.

Celem projektowanych zmian jest takie zorganizowanie systemu kierowania i dowodzenia Siłami Zbrojnymi, aby za każdą strategiczną funkcję tego dowodzenia odpowiadał odrębny organ podporządkowany bezpośrednio Ministrowi Obrony Narodowej.

Aktualne struktury kierowania i dowodzenia Siłami Zbrojnymi wyglądają następująco:

Szef Sztabu Generalnego Wojska Polskiego dowodzi w imieniu Ministra Obrony Narodowej Siłami Zbrojnymi w czasie pokoju. Do jego zadań należy perspektywiczne, wieloletnie planowanie i programowanie strategiczne, dowodzenie ogólne oraz dowodzenie operacyjne Siłami Zbrojnymi.

Rodzajami Sił Zbrojnych dowodzą – podporządkowani Szefowi Sztabu Generalnego Wojska Polskiego – Dowódca Wojsk Lądowych, Dowódca Sił Powietrznych, Dowódca Marynarki Wojennej oraz Dowódca Wojsk Specjalnych. Zadaniem Dowódcy Operacyjnego Sił Zbrojnych, który również jest podporządkowany Szefowi Sztabu Generalnego Wojska Polskiego, jest dowodzenie operacyjne częścią Sił Zbrojnych, wydzieloną z Wojsk Lądowych, Sił Powietrznych oraz Marynarki Wojennej, i podporządkowaną mu decyzją Ministra Obrony Narodowej w celu przeprowadzenia operacji. W zakresie dotyczącym Wojsk Specjalnych uprawnienie to przysługuje Dowódcy Wojsk Specjalnych.

Ponadto w strukturze Sił Zbrojnych funkcjonuje stanowisko Szefa Inspektoratu Wsparcia Sił Zbrojnych, który odpowiada za organizowanie systemu wsparcia logistycznego Sił Zbrojnych

i kierowanie tym systemem. Podlegają mu związki organizacyjne i jednostki wojskowe niewchodzące do struktur rodzajów Sił Zbrojnych.

Projekt przewiduje połączenie odrębnych dziś dowództw rodzajów Sił Zbrojnych w Dowództwo Generalne Rodzajów Sił Zbrojnych, co ma na celu sprostanie wyzwaniom współczesnego środowiska bezpieczeństwa (praktycznie wszystkie współczesne operacje to operacje połączone, prowadzone z udziałem różnych rodzajów Sił Zbrojnych).

W efekcie wprowadzonych zmian za planowanie strategicznego użycia Sił Zbrojnych, doradztwo strategiczne oraz nadzór strategiczny odpowiadałby Szef Sztabu Generalnego Wojska Polskiego, za dowodzenie ogólne – Dowódca Generalny Rodzajów Sił Zbrojnych, a za dowodzenie operacyjne – Dowódca Operacyjny Rodzajów Sił Zbrojnych.

Idea „połączenia" zakłada dowodzenie przez Dowódcę Generalnego Rodzajów Sił Zbrojnych formacjami różnych rodzajów Sił Zbrojnych w ramach ich ogólnego funkcjonowania, a przez Dowódcę Operacyjnego Rodzajów Sił Zbrojnych – formacjami różnych rodzajów Sił Zbrojnych wydzielonych do jego dyspozycji do realizacji operacji wojennych, operacji dotyczących sytuacji kryzysowych oraz misji pokojowych.

W sensie formalnoprawnym Dowódca Generalny oraz Dowódca Operacyjny będą dowódcami rodzajów Sił Zbrojnych. Zgodnie z art. 134 ust. 3 Konstytucji Rzeczypospolitej Polskiej ich mianowanie, tak jak mianowanie Szefa Sztabu Generalnego Wojska Polskiego, leży w kompetencjach Prezydenta Rzeczypospolitej Polskiej. Jest to jedno z uprawnień Prezydenta wynikających z tytułu sprawowania najwyższego zwierzchnictwa nad Siłami Zbrojnymi.

Projekt przewiduje zasadnicze zmiany w ustawie z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 1996 r. Nr 10, poz. 56, z późn. zm.) oraz ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2012 r. poz. 461, z późn. zm.). Zmiany te obejmują:

1. Określenie organów, w tym organów dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej, przy pomocy których Minister Obrony Narodowej wykonuje swoje zadania (art. 1 pkt 3 projektu).

   Projekt przewiduje rozdzielenie funkcji planistycznych, funkcji dowodzenia ogólnego i funkcji dowodzenia operacyjnego Siłami Zbrojnymi. W rezultacie Sztab Generalny Wojska Polskiego zostanie przekształcony w organ planowania, doradztwa strategicznego i nadzoru, a obecne organy dowodzenia zostaną zastąpione dwoma dowództwami strategicznymi: jednym odpowiedzialnym za ogólne dowodzenie wojskami (Dowódca Generalny Rodzajów Sił Zbrojnych) i drugim odpowiedzialnym za dowodzenie operacyjne w czasie wojen, sytuacji kryzysowych i dowodzenie wojskami poszczególnych rodzajów Sił Zbrojnych wydzielonymi do zagranicznych misji pokojowych (Dowódca Operacyjny Rodzajów Sił Zbrojnych). Ponieważ wymienione podmioty będą odpowiedzialne za znaczny zakres zadań Ministra Obrony Narodowej, konieczne jest właściwe ich umiejscowienie w systemie prawnym, obok wskazanych obecnie organów, przy pomocy których Minister Obrony Narodowej wykonuje swoje zadania.

2. Powierzenie dowodzenia Siłami Zbrojnymi dwóm organom, z uwzględnieniem rozdzielenia ich funkcji na dowodzenie ogólne i operacyjne oraz zasady „połączenia" (art. 1 pkt 3 oraz art. 3 pkt 1 projektu).

   Minister Obrony Narodowej będzie kierował całokształtem działalności Sił Zbrojnych Rzeczypospolitej Polskiej przy pomocy Dowódcy Generalnego Rodzajów Sił Zbrojnych i Dowódcy Operacyjnego Rodzajów Sił Zbrojnych. Funkcjonujące obecnie dowództwa rodzajów Sił Zbrojnych zostaną zastąpione dwoma dowództwami strategicznymi – jednym odpowiedzialnym za ogólne dowodzenie wojskami (Dowództwo Generalne Rodzajów Sił Zbrojnych) i drugim odpowiedzialnym za dowodzenie operacyjne w czasie

wojen, w sytuacjach kryzysowych i za dowodzenie siłami wydzielonymi do zagranicznych misji pokojowych (Dowództwo Operacyjne Rodzajów Sił Zbrojnych).

Wskazani wyżej dowódcy będą faktycznie dowodzić istniejącymi rodzajami Sił Zbrojnych, tj. Wojskami Lądowymi, Siłami Powietrznymi, Marynarką Wojenną i Wojskami Specjalnymi. Z tego też względu konieczne jest ustawowe umocowanie ich jako dowódców rodzajów Sił Zbrojnych.

3. Wskazanie podmiotów bezpośrednio podległych Ministrowi Obrony Narodowej (art. 1 pkt 3 projektu).

   Ministrowi Obrony Narodowej podlegaliby bezpośrednio: Szef Sztabu Generalnego Wojska Polskiego, Dowódca Generalny Rodzajów Sił Zbrojnych i Dowódca Operacyjny Rodzajów Sił Zbrojnych. Ponadto wskazuje się, że podmiotami, które podlegają Ministrowi Obrony Narodowej są Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego.

4. Usytuowanie Szefa Sztabu Generalnego Wojska Polskiego jako organu pomocniczego Ministra Obrony Narodowej w kierowaniu całokształtem działalności Sił Zbrojnych. Uchylenie jego kompetencji dotyczących dowodzenia w imieniu Ministra Obrony Narodowej w czasie pokoju Siłami Zbrojnymi Rzeczypospolitej Polskiej, zniesienie obowiązku opiniowania lub wnioskowania przez ten organ decyzji w sprawach związanych ze strukturą organizacyjną i działalnością Sił Zbrojnych Rzeczypospolitej Polskiej oraz określenie na nowo jego zakresu zadań (art. 1 pkt 3 i 5 projektu).

   Z uwagi na rozdzielenie funkcji planowania strategicznego, dowodzenia ogólnego oraz dowodzenia operacyjnego, kierowanie całokształtem działalności Sił Zbrojnych Minister Obrony Narodowej będzie realizował przy pomocy Dowódcy Generalnego Rodzajów Sił Zbrojnych oraz Dowódcy Operacyjnego Rodzajów Sił Zbrojnych. Natomiast Szef Sztabu Generalnego Wojska Polskiego zostanie jego organem pomocniczym w tych sprawach, który będzie wykonywał swoje zadania (tak jak obecnie) przy pomocy Sztabu Generalnego Wojska Polskiego.

5. Określenie pozycji ustrojowej Dowódcy Generalnego Rodzajów Sił Zbrojnych w strukturze dowodzenia Siłami Zbrojnymi (art. 3 pkt 3 projektu).

   Dowódca Generalny Rodzajów Sił Zbrojnych będzie dowodził rodzajami Sił Zbrojnych i odpowiadał za ich przygotowywanie do realizacji zadań operacyjnych, z wyłączeniem części Sił Zbrojnych, o których mowa w art. 3 pkt 3 projektu (w zakresie dodawanego art. 11a ust. 1 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej). Dowódca Generalny Rodzajów Sił Zbrojnych będzie wykonywał swoje zadania przy pomocy Dowództwa Generalnego Rodzajów Sił Zbrojnych, którego szczegółowy zakres działania, siedzibę i strukturę organizacyjną określi Minister Obrony Narodowej w drodze zarządzenia.

6. Określenie pozycji ustrojowej Dowódcy Operacyjnego Rodzajów Sił Zbrojnych w strukturze dowodzenia Siłami Zbrojnymi (art. 3 pkt 3 projektu).

   Dowódca Operacyjny Rodzajów Sił Zbrojnych będzie odpowiadał za operacyjne dowodzenie częścią Sił Zbrojnych podporządkowaną mu na podstawie decyzji Ministra Obrony Narodowej. Dowódca Operacyjny Rodzajów Sił Zbrojnych będzie wykonywał swoje zadania przy pomocy Dowództwa Operacyjnego Rodzajów Sił Zbrojnych, którego szczegółowy zakres działania, siedzibę i strukturę organizacyjną określi Minister Obrony Narodowej w drodze zarządzenia.

7. Usprawnienie mechanizmu przechodzenia ze stanu „P" na stan „W" (w aspekcie personalnym) dzięki dodaniu podstawy prawnej umożliwiającej Prezydentowi Rzeczypospolitej Polskiej wskazanie osoby przewidzianej do mianowania na stanowisko Naczelnego Dowódcy Sił Zbrojnych na czas wojny (art. 3 pkt 2 projektu).

Zgodnie z art. 134 ust. 4 Konstytucji Rzeczypospolitej Polskiej na czas wojny Prezydent Rzeczypospolitej Polskiej mianuje Naczelnego Dowódcę Sił Zbrojnych. Aby umożliwić właściwe przygotowanie do działania w czasie wojny Naczelnego Dowództwa Sił Zbrojnych, Prezydent będzie wskazywał, na wniosek Prezesa Rady Ministrów, osobę przewidzianą do mianowania na stanowisko Naczelnego Dowódcy Sił Zbrojnych na czas wojny.

Projektowana nowelizacja nie zmieni procedur dotyczących mianowania Naczelnego Dowódcy Sił Zbrojnych, które wynikają wprost z przywołanego wyżej przepisu ustawy zasadniczej. Pozwoli natomiast stworzyć właściwe mechanizmy przechodzenia z systemu pokojowego na wojenny system dowodzenia oraz przygotować określone osoby do realizacji zadań wynikających ze sprawowania tej niezwykle ważnej funkcji, w tym w ramach krajowych ćwiczeń systemu obronnego państwa.

Pozostałe propozycje zmian w ustawie o urzędzie Ministra Obrony Narodowej są konsekwencją zmian, jakie zaszły w systemie prawnym od wejścia w życie tej ustawy. W rezultacie proponuje się:

1. nowe brzmienie przepisu art. 1 ust. 1 ustawy o urzędzie Ministra Obrony Narodowej;
2. zastąpienie dotychczasowych wyrażeń „organy administracji państwowej" wyrażeniami „organy administracji rządowej" stosownie do terminologii zawartej m.in. w ustawie z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie – por. art. 1 pkt 2 projektu.

Na skutek wprowadzenia zmian w strukturze dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej (zastąpienie dotychczasowych dowódców Wojsk Lądowych, Sił Powietrznych, Marynarki Wojennej i Wojsk Specjalnych oraz Dowódcy Operacyjnego Sił Zbrojnych RP Dowódcą Generalnym Rodzajów Sił Zbrojnych oraz Dowódcą Operacyjnym Rodzajów Sił Zbrojnych) konieczne się stało wprowadzenie zmian aktualizacyjnych (w zakresie terminologii) w następujących ustawach:

1. ustawie z dnia 1 grudnia 1961 r. o izbach morskich;
2. ustawie z dnia 12 października 1990 r. o ochronie granicy państwowej;
3. ustawie z dnia 23 września 1999 r. o zasadach pobytu wojsk obcych na terytorium Rzeczypospolitej Polskiej oraz zasadach ich przemieszczania się przez to terytorium;
4. ustawie z dnia 11 kwietnia 2003 r. o świadczeniach odszkodowawczych przysługujących w razie wypadków i chorób pozostających w związku ze służbą wojskową;
5. ustawie z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych;
6. ustawie z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
7. ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich;
8. ustawie z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim.

Z uwagi na zakres i istotę zmian projekt przewiduje następujące przepisy dostosowujące i przejściowe:

1. z dniem wejścia w życie ustawy likwiduje się Dowództwo Wojsk Lądowych, Dowództwo Sił Powietrznych, Dowództwo Marynarki Wojennej i Dowództwo Wojsk Specjalnych;
2. z dniem wejścia w życie ustawy Minister Obrony Narodowej utworzy Dowództwo Generalne Rodzajów Sił Zbrojnych;
3. z dniem wejścia w życie ustawy Dowództwo Operacyjne Sił Zbrojnych staje się Dowództwem Operacyjnym Rodzajów Sił Zbrojnych;

4. z dniem wejścia w życie ustawy Dowódca Generalny Rodzajów Sił Zbrojnych wstępuje w prawa i obowiązki dowódców Wojsk Lądowych, Sił Powietrznych, Marynarki Wojennej i Wojsk Specjalnych, a Dowódca Operacyjny Rodzajów Sił Zbrojnych wstępuje w prawa i obowiązki Dowódcy Operacyjnego Sił Zbrojnych;
5. sprawy wszczęte i niezakończone przed dniem wejścia w życie ustawy prowadzone przez:
    a. dowódców Wojsk Lądowych, Sił Powietrznych, Marynarki Wojennej i Wojsk Specjalnych przejmuje Dowódca Generalny Rodzajów Sił Zbrojnych,
    b. Dowódcę Operacyjnego Sił Zbrojnych przejmuje Dowódca Operacyjny Rodzajów Sił Zbrojnych;
6. z dniem wejścia w życie ustawy część Sił Zbrojnych Rzeczypospolitej Polskiej podporządkowana Dowódcy Operacyjnemu Sił Zbrojnych na podstawie dotychczasowych przepisów staje się częścią Sił Zbrojnych Rzeczypospolitej Polskiej podporządkowaną Dowódcy Operacyjnemu Rodzajów Sił Zbrojnych.

Przewiduje się, że projektowana regulacja wejdzie w życie z dniem 1 stycznia 2014 r.

Projekt ustawy nie zawiera norm technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039, z późn. zm.), dlatego nie podlega notyfikacji ani obowiązkowi przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu w celu uzyskania opinii.

Przedmiot projektowanych regulacji nie jest objęty zakresem prawa Unii Europejskiej.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414, z późn. zm.) projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej na stronach internetowych Ministerstwa Obrony Narodowej oraz na stronach internetowych Rządowego Centrum Legislacji w Rządowym Procesie Legislacyjnym. W trakcie prac nad projektem nie zgłosiły się podmioty zainteresowane pracami nad nim.

OCENA SKUTKÓW REGULACJI

1. Podmioty, na które oddziałuje projekt aktu prawnego

    Podmiotami, na które będzie oddziaływała projektowana ustawa są: Ministerstwo Obrony Narodowej, jednostki organizacyjne podległe lub nadzorowane przez Ministra Obrony Narodowej oraz Siły Zbrojne Rzeczypospolitej Polskiej.

    Projektowana ustawa oddziaływać będzie także na żołnierzy zawodowych i pracowników wojska zajmujących stanowiska służbowe w jednostkach organizacyjnych objętych projektowanymi zmianami oraz na członków korpusu służby cywilnej (ksc) zatrudnionych w komórkach organizacyjnych Ministerstwa Obrony Narodowej.

2. Konsultacje społeczne

    Projekt założeń projektu ustawy, na podstawie którego opracowano przedstawiony projekt ustawy, był przedmiotem konsultacji społecznych z:

    1) Konwentem Dziekanów Korpusu Oficerów Zawodowych Wojska Polskiego;
    2) Niezależnym Samorządnym Związkiem Zawodowym Pracowników Wojska, ul. Koszykowa 79a, 00-909 Warszawa;

3) Sekcją Krajową Pracowników Cywilnych MON NSZZ „Solidarność”, ul. Śmidowicza 48, 81-127 Gdynia;

4) Związkiem Zawodowym Pracowników Przemysłu Poligraficznego, ul. Bracka 23/44, 00-028 Warszawa;

5) Zarządem Krajowym Ogólnopolskiego Pracowniczego Związku Zawodowego „Konfederacja Pracy”, ul. Kopernika 36/40, 00-924 Warszawa;

6) Zarządem Głównym Związku Zawodowego Militaria, ul. 1-go Sierpnia 24/13, 02-134 Warszawa;

7) Stowarzyszeniem Niezależne Forum o Wojsku, ul. Powstańców Wielkopolskich 7/4, 06-413 Ciechanów;

8) Radą Służby Cywilnej, Al. Ujazdowskie 1/3, 00-583 Warszawa.

Ponadto projekt został umieszczony w Biuletynie Informacji Publicznej na stronie internetowej Rządowego Centrum Legislacji.

W ramach konsultacji społecznych, podczas szeregu spotkań, przedstawiano informację na temat projektu założeń projektu ustawy o zmianie ustawy o urzędzie Ministra Obrony Narodowej i niektórych innych ustaw z podkreśleniem potrzeby podjęcia reformy struktur dowodzenia, istoty proponowanej zmiany, oczekiwanych korzyści dla systemu zarządzania, kierowania i dowodzenia Siłami Zbrojnymi RP oraz wymagań legislacyjnych projektu. Przedstawiano także zidentyfikowane koszty społeczne zmiany oraz rozważane sposoby ich łagodzenia.

Uczestników konsultacji społecznych zapewniono, iż w stosunku do wszystkich pracowników, których dotknie zmiana, priorytetem będzie wykorzystanie potencjału pracowniczego zatrudnionego dziś w Ministerstwie Obrony Narodowej i w reformowanych strukturach dowodzenia.

W stosunku do żołnierzy zawodowych, pracowników wojska oraz członków korpusu Służby Cywilnej zatrudnionych w Ministerstwie Obrony Narodowej planuje się dokonanie przesunięć (alokacji) na inne stanowiska w nowo tworzonej strukturze. Część zatrudnionych uzyskało już prawa emerytalne. Niestety, w stosunku do części z nich nieuniknione będą także zwolnienia w ramach zwolnień grupowych.

W toku konsultacji zwracano także uwagę czynnika społecznego na skalę corocznych odejść ze służby żołnierzy zawodowych i wskazano, iż w stosunku do tych wielkości przewidywane zmiany nie stanowią zagrożenia wzrostem rocznego poziomu zwolnień. Jednocześnie projektowana zmiana umożliwi w Siłach Zbrojnych RP poprawę proporcji liczby oficerów starszych i oficerów młodszych i podoficerów w jednostkach wojskowych.

3. Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego

1) Zmniejszenie zatrudnienia pracowników wojska i ksc

i. w stosunku do pracowników wojska przewiduje się, że zostanie im zaproponowane inne miejsce zatrudnienia. Jednak ze względu na możliwą konieczność zmiany zarówno charakteru, jak i miejsca pracy – możliwe jest zmniejszenie zatrudnienia pracowników o 525 stanowisk (w tym 16 członków ksc), które skutkować będzie oszczędnością środków na wynagrodzenia (bez pochodnych) w skali roku na poziomie około 19 115 tys. zł. Do szacunków przyjęto średnie wynagrodzenie wraz z dodatkowym wynagrodzeniem rocznym wyliczone w oparciu o dane prezentowane w sprawozdaniu o zatrudnieniu i wynagrodzeniu Rb 70 za III kw. 2012 r.,

ii. wymuszone zwolnienia pracowników mogą generować zwiększenie ilości wypłat nagród jubileuszowych i odpraw emerytalnych – wg szacunków może to dotyczyć około 20% zwalnianych (około 100 pracowników). Szacunkowy koszt wypłat zwiększonej ilości nagród jubileuszowych i odpraw emerytalnych (w ramach funduszu wynagrodzeń pracowników) w roku zwolnienia pracowników – około 1 600 tys. zł (przy założeniu, że średnie wynagrodzenie w roku 2012 bez dodatkowych należności, nagród uznaniowych i dodatkowego wynagrodzenia rocznego wynosiło 2 625 zł),

iii. rozwiązanie z pracownikami stosunków pracy z przyczyn niedotyczących pracowników generuje dodatkowe jednorazowe koszty w postaci odprawy pieniężnej. Przy założeniu, że zwalnianym pracownikom wypłacone zostaną odprawy w wysokości trzymiesięcznego wynagrodzenia (wyliczone z uwzględnieniem średniego wynagrodzenia – jak wyżej – na poziomie 2 625 zł) koszt odpraw będzie kształtował się na poziomie około 3 300 tys. zł.

2) Zmiany w stanach osobowych żołnierzy zawodowych

W 2014 r. może zrezygnować z alokacji na innych stanowiskach służbowych i w konsekwencji zostanie zwolnionych 450 żołnierzy zawodowych, z których wszyscy będą posiadali prawo do korzystania z pomocy rekonwersyjnej w zakresie przekwalifikowania zawodowego w wysokości najwyższej, tj. 300% przysługującego limitu1) – obecnie 5 625 zł. W związku z powyższym istnieje konieczność zaplanowania dodatkowych środków na wskazane działania rekonwersyjne w wysokości ok. 2 000 tys. zł – 2 500 tys. zł, przy założeniu, że z wojska odejdzie jedynie planowana liczba żołnierzy.

Wysokość limitu określono na poziomie 75% najniższego uposażenia zasadniczego żołnierza zawodowego obowiązującego w dniu 1 stycznia roku kalendarzowego, w którym zainteresowany wystąpi z wnioskiem o udzielenie pomocy w przekwalifikowaniu zawodowym.

Jednocześnie należy wskazać, że pozostała liczba żołnierzy zawodowych, tj. 2.270, którzy mają znaleźć zatrudnienie w nowo powstałych strukturach, może z takiej możliwości nie skorzystać (z różnych powodów). W takim przypadku istnieje konieczność zabezpieczenia dodatkowych, zwiększonych środków na rekonwersję, których wysokość obecnie jest trudna do oszacowania.

Przeprowadzona kalkulacja kosztów wejścia w życie projektowanej regulacji w zakresie wydatków osobowych (poza wynagrodzeniami) pokazała, że w 2014 r. wyniosą one ok. 100 604 tys. zł.

Z przeprowadzonych kalkulacji wynika, iż koszt wejścia w życie przedmiotowego projektu ustawy w 2014 r. w zakresie: uposażeń żołnierzy, dodatkowego uposażenia rocznego, należności płaconych przy przejściu na emeryturę, wyniesie ok. 104 358 tys. zł.

Konieczne wydatki zostaną sfinansowane w ramach budżetu MON (część 29 budżetu państwa).

4. Wpływ regulacji na rynek pracy

Możliwe zwolnienie z resortu obrony narodowej 525 pracowników wojska (w tym członków ksc) nie będzie miało znaczącego wpływu na rynek pracy.

Jednak, w przypadku gdy jednorazowo większe zwolnienia pracowników wojska nastąpią w jednostce, bądź instytucji wojskowej znajdującej się w regionie, gdzie rynek pracy jest trudny a bezrobocie znaczne – mogą mieć one wpływ na lokalny rynek pracy.

Wejście w życie projektowanych rozwiązań może zwiększyć liczbę osób o specyficznych specjalnościach poszukujących pracy.

Województwa, w których przewidywany jest wzrost liczby osób bezrobotnych: małopolskie, pomorskie, kujawsko-pomorskie.

5. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw

   Regulacja nie wpłynie na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw.

6. Wpływ regulacji na sytuację i rozwój regionalny

   Proponowane regulacje prawne nie będą miały wpływu na sytuację gospodarczą i rozwój regionalny.

   Proponowane regulacje nie będą miały także wpływu na ochronę środowiska naturalnego.

UZASADNIENIE
DO PRZYGOTOWANEGO W BBN PROJEKTU USTAWY WS. FINANSOWANIA BUDOWY OBRONY POWIETRZNEJ, W TYM PRZECIWRAKIETOWEJ

24 września 2012 r. Prezydent RP Bronisław Komorowski przesłał do Sejmu RP przygotowany w BBN projekt ustawy zmieniającej ustawę o przebudowie i modernizacji technicznej oraz finansowaniu Sił Zbrojnych RP.

Celem ustawy było wprowadzenie – zewnętrznego w stosunku do wojskowych procesów planistycznych – mechanizmu konsekwentnego przekazywania środków finansowych na realizację projektu bydowy głównego priorytetu modernizacyjnego Sił Zbrojnych RP, tj obrony powietrznej, w tym przeciwrakietowej.

Ustawa została przyjęta przez Sejm 22 lutego 2013 r. i podpisana przez Prezydenta RP 12 kwietnia 2013 r.

BIURO BEZPIECZEŃSTWA NARODOWEGO

24 września 2012 r.

UZASADNIENIE DO PRZYGOTOWANEGO W BBN PROJEKTU USTAWY ZMIENIAJĄCEJ USTAWĘ O PRZEBUDOWIE I MODERNIZACJI TECHNICZNEJ ORAZ FINANSOWANIU SIŁ ZBROJNYCH RP, MAJĄCEJ NA CELU USTANOWIENIE FINANSOWANIA BUDOWY OBRONY POWIETRZNEJ, W TYM PRZECIWRAKIETOWEJ

Zasadniczym celem proponowanej zmiany w ustawie z dnia 25 maja 2001 r. o przebudowie i modernizacji technicznej oraz finansowaniu Sił Zbrojnych Rzeczypospolitej Polskiej (Dz. U. z 2009 r. Nr 67, poz. 570, z późn. zm.) jest wzmocnienie bezpieczeństwa państwa poprzez podwyższenie minimalnego poziomu finansowania potrzeb obronnych Rzeczypospolitej Polskiej z obecnego 1,95 % do 2 % Produktu Krajowego Brutto z roku poprzedniego - zgodnie z zaleceniami Sojuszu Północnoatlantyckiego.

Kryzys na Ukrainie i rozwój sytuacji polityczno-wojskowej w Europie Wschodniej wskazuje bowiem, że Polska w najbliższej perspektywie może stać się obiektem nacisków, presji lub szantażu polityczno-militarnego. W takiej sytuacji konieczne jest uwzględnienie wspomnianych uwarunkowań zewnętrznych w procesie przygotowań obronnych, co wiąże się z potrzebą zwiększenia nakładów finansowych.

Członkostwo Polski w NATO jest bardzo istotnym elementem naszego bezpieczeństwa. Jednakże Polska, aby móc skorzystać z potencjalnej pomocy militarnej NATO, powinna posiadać nowoczesną infrastrukturę obronną, pozwalającą na przyjęcie i pobyt wojsk sojuszniczych na terytorium Rzeczypospolitej Polskiej, a także wzmacniającą strategiczną odporność kraju na agresję. Istniejąca infrastruktura obronna, w szczególności we wschodniej części kraju, wymaga rozbudowy i modernizacji. Ze względu na kosztowność i czas realizacji tych przedsięwzięć wymagane jest ich stabilne finansowanie w wieloletniej perspektywie.

Innym priorytetowym zadaniem wymagającym stabilnego finansowania jest wyposażenie systemu obronnego Rzeczypospolitej w systemy bezzałogowe w ramach tzw. "trzeciej informatycznej fali" modernizacji technicznej Sił Zbrojnych i innych służb państwowych działających na rzecz bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Dotyczy to wszystkich rodzajów techniki bezzałogowej, wykorzystywanej w powietrzu, na lądzie, na wodzie i pod wodą.

Warto zauważyć, że problem ten został podniesiony podczas przeprowadzonego w latach 2010-2012 Strategicznego Przeglądu Bezpieczeństwa Narodowego. W Białej Księdze Bezpieczeństwa Narodowego wskazano, iż "potrzebne jest wprowadzenie do wyposażenia sił zbrojnych najnowocześniejszych technologicznie zinformatyzowanych systemów walki i wsparcia, stosowanych w rozpoznaniu, walce w cyberprzestrzeni, dowodzeniu, kierowaniu systemami

uzbrojenia, środków precyzyjnego rażenia, zdalnego kierowania systemami bezzałogowymi, a także robotach".

Biorąc powyższe pod uwagę proponuje się, aby dodatkowe środki, wynikające ze zwiększenia budżetu obronnego do 2 % PKB, były corocznie przeznaczane na finansowanie obydwu wspomnianych wyżej bardzo istotnych z punktu widzenia bezpieczeństwa narodowego zadań, znacznie podnoszących narodowe możliwości obronne i zdolności do przyjęcia sojuszniczych sił wzmocnienia.

Dla osiągnięcia wszystkich w/w celów modernizacyjnych Sił Zbrojnych RP proponuje się nowelizację art. 7 ust. 1 ustawy o przebudowie i modernizacji technicznej oraz finansowaniu Sił Zbrojnych Rzeczypospolitej Polskiej, poprzez stałe podwyższenie minimalnych nakładów na potrzeby obronne do 2 % Produktu Krajowego Brutto z roku poprzedniego oraz dodanie ust. 2b, stanowiącego, że na rozbudowę i modernizację infrastruktury na potrzeby obronne państwa oraz wyposażenie systemu obronnego Rzeczypospolitej Polskiej w systemy bezzałogowe przeznacza się corocznie, z ogólnych wydatków obronnych, wydatki w wysokości co najmniej 0,05 % Produktu Krajowego Brutto z roku poprzedniego.

Na podstawie obecnych prognoz dotyczących kształtowania się PKB ocenia się, że przyjęcie proponowanego rozwiązania pozwoliłoby pozyskać corocznie na ww. cel kwotę około 800 mln zł. Środki te powinny umożliwić podniesienie w znaczny sposób zdolności Sił Zbrojnych RP poprzez wprowadzenie nowoczesnych bezzałogowców do różnych form ich działalności, jak też znacząco zwiększyć możliwość przyjęcia i funkcjonowania sojuszniczych sił wzmocnienia w razie potrzeby ich użycia na terytorium Rzeczypospolitej Polskiej na podstawie art. 5 Traktatu Północnoatlantyckiego.

Projekt nie jest objęty zakresem prawa Unii Europejskiej.

STRATEGICZNY PRZEGLĄD BEZPIECZEŃSTWA NARODOWEGO – GŁÓWNE WNIOSKI I REKOMENDACJE DLA POLSKI

W latach 2010-2012 przeprowadzony został pierwszy polski Strategiczny Przegląd Bezpieczeństwa Narodowego. Prace, które skupiły ponad 200 ekspertów, koordynowane były przez Biuro Bezpieczeństwa Narodowego. Rezultaty SPBN zostały przyjęte przez Radę Bezpieczeństwa Narodowego 8 listopada 2012 r.

Przedmiotowe opracowanie, zawierające głowne wnioski oraz rekomendacje z prac, zostało opublikowane 12 grudnia 2012 r.

Pełne, jawne rezultaty Przeglądu zostały natomiast zawarte w Białej Księdze Bezpieczeństwa Narodowego RP, opublikowanej w maju 2013 r.

BIURO BEZPIECZEŃSTWA NARODOWEGO

12 grudnia 2012 r.

STRATEGICZNY PRZEGLĄD BEZPIECZEŃSTWA NARODOWEGO – GŁÓWNE WNIOSKI I REKOMENDACJE DLA POLSKI

Słowo wstępne

Strategiczny Przegląd Bezpieczeństwa Narodowego (SPBN) był pierwszym tego typu przedsięwzięciem w Polsce. Dokonano w nim całościowej oceny stanu bezpieczeństwa narodowego oraz sformułowano strategiczne wnioski dotyczące pożądanych kierunków i sposobów działania państwa w tej dziedzinie oraz przygotowania systemu bezpieczeństwa narodowego.

Przegląd przeprowadzono w czterech etapach: samoidentyfiacji strategicznej, obejmującej diagnozę państwa jako podmiotu bezpieczeństwa; oceny strategicznego środowiska bezpieczeństwa; formułowania koncepcji działań strategicznych, określającej sposób osiągania celów strategicznych w danych warunkach (środowisku) bezpieczeństwa oraz formułowania koncepcji przygotowań strategicznych, określającej sposób utrzymywania i transformacji systemu bezpieczeństwa narodowego.

Rezultaty Przeglądu zostały zawarte w Raporcie Komisji, który przedstawiono Prezydentowi RP Bronisławowi Komorowskiemu. 8 listopada 2012 r. przyjęła je jednomyślnie Rada Bezpieczeństwa Narodowego.

1. Diagnoza Polski jako podmiotu bezpieczeństwa. Interesy narodowe i cele strategiczne

Geopolityczne położenie Polski między Zachodem a Wschodem jest najważniejszym strategicznym czynnikiem kształtującym od wieków tożsamość narodową i państwowość polską oraz wynikające z nich interesy narodowe i cele strategiczne.

Składniki potencjału strategicznego:

- potencjał ustrojowo-polityczny – zasady ustrojowe Konstytucji RP stwarzają ramy do określenia interesów i celów strategicznych w dziedzinie bezpieczeństwa;
- potencjał obronny – adekwatny do prognozowanych zagrożeń i wyzwań. Największa jego część, Siły Zbrojne RP, wymaga dokończenia profesjonalizacji, zwiększenia zdolności operacyjnych poprzez wprowadzenie nowoczesnego uzbrojenia i wyposażenia do wojsk, podniesienia poziomu wyszkolenia oraz konsolidacji organizacyjnej;
- potencjał ochronny – stoi przed szeregiem trudnych wyzwań. Należą do nich m.in.: szeroko rozumiana przestępczość zorganizowana, terroryzm (w tym cyberterroryzm) oraz nielegalna migracja. Nadmierna liczba służb i rozproszony nadzór komplikują koordynację oraz osłabiają spójność działań służb i straży;

- potencjały społeczny i gospodarczy w zróżnicowany sposób wpływają na definiowanie interesów narodowych oraz celów strategicznych w dziedzinie bezpieczeństwa. Zrównoważony rozwój społeczno-gospodarczy państwa powinien zapewnić odpowiednie zasoby i zdolności dla systemu bezpieczeństwa państwa. Czynnikiem pozytywnym jest rozwój gospodarki. Ograniczająco działa stan finansów publicznych, wynikający z ogólnej nierównowagi sektora finansowego. Negatywny wpływ może mieć sytuacja demograficzna kraju.

2. Ocena i prognoza środowiska bezpieczeństwa. Scenariusze kształtowania się warunków bezpieczeństwa

Wymiary środowiska bezpieczeństwa:

- globalny – pozytywny (postęp polityczny, społeczny i gospodarczy) i negatywny wpływ globalizacji (fragmentacja bezpieczeństwa); wzrost zapotrzebowania na surowce, żywność i wodę; istnienie konflktogennych ognisk zapalnych; erozja reżimu nieproliferacji; zagrożenia terrorystyczne i ich przeniesienie do cyberprzestrzeni oraz słabnięcie roli organizacji międzynarodowych;
- regionalny – cztery determinanty bezpieczeństwa: NATO, UE, strategiczna obecność USA,relacje z Rosją. NATO podstawowym gwarantem bezpieczeństwa Polski; wyzwanie – konsolidacja Sojuszu wokół gwarancji obrony zbiorowej. UE: zagrożenie – kryzys strefy euro, wyzwanie – rewitalizacja WPBiO. USA: wyzwanie – utrzymanie zaangażowania w Europie mimo strategicznego przesunięcia ku regionowi Azji i Pacyfiku. Rosja: szansa i wyzwanie – budowanie kooperatywnego bezpieczeństwa i partnerstwa z Polską i Sojuszem; ryzyko/zagrożenie – kryzys wzajemnego zaufania. Kryzysy – obszar poradziecki i Bałkany Zachodnie;
- krajowy – zagrożenie militarne na dużą skalę mało prawdopodobne, istnieją jednak ryzykazwiązane z możliwością grożenia użyciem przemocy. Zagrożenia: dekapitalizacja infrastruktury, sytuacja demograficzna. Wyzwania: zapewnienie niezakłóconego rozwoju gospodarczego, stabilnej sytuacji finansowej i dalekosiężnej, spójnej polityki społecznej. Szansa: eksploatacja gazu łupkowego.

Scenariusze kształtowania się warunków bezpieczeństwa:

- integracyjny – z przewagą pozytywnych i pożądanych zjawisk i tendencji;
- dezintegracyjny – z przewagą niekorzystnych i niebezpiecznych zjawisk zewnętrznych i wewnętrznych;
- ewolucyjny – kontynuacja względnej równowagi negatywnych i pozytywnych zjawisk.

3. Strategia operacyjna (koncepcja działań strategicznych) – możliwe opcje

Opcje strategii operacyjnej:

- opcja maksymalnego umiędzynarodowienia działań na rzecz bezpieczeństwa Polski, związana z przesunięciem priorytetów na działania pozamilitarne;
- opcja autarkii strategicznej (samodzielności i samowystarczalności) – zakłada zdecydowane wzmocnienie samodzielności działania państwa w sferze bezpieczeństwa w kontekście kryzysu kooperatywnej polityki bezpieczeństwa w Europie i we wspólnocie transatlantyckiej;
- opcja zrównoważonego umiędzynarodowienia i usamodzielnienia bezpieczeństwa Polski – zakłada wzmacnianie więzi sojuszniczych oraz relacji dwustronnych z najważniejszymi partnerami i uwiarygodnienie przez to zewnętrznych filarów

bezpieczeństwa z jednoczesną gotowością do samodzielnego działania w sytuacjach, w których pełna wiarygodność sojusznicza może okazać się problematyczna.

Priorytety strategii operacyjnej:

- utrzymanie własnej determinacji i gotowości do działania w pełnym spektrum dziedzin, obszarów i sektorów bezpieczeństwa narodowego, z priorytetowym traktowaniem tych, w których sojusznicze (wspólne) działanie może być utrudnione;
- umacnianie międzynarodowej wspólnoty bezpieczeństwa przez pogłębianie opartych na wspólnocie interesów procesów integracyjnych w Europie;
- wspieranie i selektywny udział w przedsięwzięciach zapobiegających powstaniu nowych źródeł zagrożeń lub rozprzestrzenianiu się już istniejących kryzysów w wymiarze ponadregionalnym.

4. Strategia preparacyjna (koncepcja przygotowania systemu bezpieczeństwa narodowego) – możliwe opcje

Opcje strategii preparacyjnej:

- opcja umiędzynarodowienia systemu bezpieczeństwa narodowego podkreśla przygotowanie systemu bezpieczeństwa narodowego, którego priorytetem jest maksymalne wykorzystanie szans wynikających ze współpracy międzynarodowej;
- opcja usamodzielnienia systemu bezpieczeństwa narodowego oznacza konieczność przygotowania systemu bezpieczeństwa narodowego, którego priorytetem jest maksymalizacja narodowego potencjału bezpieczeństwa;
- opcja zrównoważonego integrowania systemu bezpieczeństwa narodowego podkreśla przygotowanie systemu bezpieczeństwa narodowego do wykorzystywania zarówno szans wynikających ze współpracy międzynarodowej, jak i racjonalnie umacnianych zdolności sukcesywnie integrowanego narodowego potencjału bezpieczeństwa.

5. Zasadnicze rekomendacje Strategicznego Przeglądu Bezpieczeństwa Narodowego

1) Operacyjne:

- za punkt wyjścia w identyfikowaniu interesów narodowych i celów strategicznych w sferze bezpieczeństwa przyjąć interesy konstytucyjne (art. 5);
- w planowaniu działań w sferze bezpieczeństwa kierować się ewolucyjnym scenariuszem kształtowania się środowiska bezpieczeństwa;
- jako główny kierunek strategii operacyjnej przyjąć opcję zrównoważonego umiędzynarodowienia i usamodzielnienia w działaniach zmierzających do zapewnienia bezpieczeństwa;
- w 2013 r. wydać nową Strategię Bezpieczeństwa Narodowego, w 2014 r. – Polityczno - strategiczną dyrektywę obronną, a w 2015 r. – uruchomić drugi SPBN. Jednocześnie, w ślad za dyrektywą, zaktualizować plan użycia Sił Zbrojnych RP oraz operacyjne plany funkcjonowania ministerstw, województw i samorządów w czasie zagrożenia i wojny, przy jednoczesnym zintegrowaniu ich z planami zarządzania kryzysowego.

2) Preparacyjne:

a) na poziomie legislacyjnym (bez zmian w obowiązującej Konstytucji) – przyjęcie lub znowelizowanie ustaw:

- kierowaniu bezpieczeństwem narodowym – cel: doprecyzowanie roli władz państwowych w zintegrowanym systemie bezpieczeństwa narodowego w czasie pokoju, zagrożenia i wojny, w tym także w stanach nadzwyczajnych; zapewnienie funkcji kierowniczo-koordynacyjnej na poziomie ponadresortowym;
- o stanie wojennym – cel: doprecyzowanie roli i kompetencji naczelnego dowódcy Sił Zbrojnych;
- o ratownictwie i ochronie ludności – cel: formalnoprawna synergia aktywności społecznej i właściwych instytucji państwa;
- o obronności (powszechnym obowiązku obrony) – cel: zastąpienie ustawy o powszechnym obowiązku obrony (uregulowanie kwestii dotyczących realizacji konstytucyjnego obowiązku obrony ojczyzny oraz zadań i zasad funkcjonowania Sił Zbrojnych RP);
- służbach specjalnych – cel: konsolidacja służb, określenie wspólnej pragmatyki, uporządkowanie kompetencji i uzyskanie interoperacyjności służb; stworzenie centrum integracji informacji specjalnych;
- o czynnościach operacyjnych – cel: zdefiiowanie procedur i kompetencji w stosowaniu technik operacyjno-rozpoznawczych;
- o urzędzie ministra obrony narodowej – cel: reforma systemu dowodzenia i kierowania SZ RP;
- o utworzeniu zintegrowanej uczelni wojskowej oraz ponadresortowej uczelni bezpieczeństwa narodowego (Akademii Bezpieczeństwa Narodowego) – cel: konsolidacja wyższego szkolnictwa wojskowego.

b) na poziomie decyzji władzy wykonawczej (Prezydent, Rada Ministrów, ministrowie):

- utrzymanie w wieloletniej perspektywie budżetu obronnego na poziomie 1,95 proc. PKB;
- konsolidacja organizacyjna i dyslokacyjna Sił Zbrojnych RP oraz konsekwentna realizacja priorytetów modernizacyjnych (obrona powietrzna, w tym przeciwrakietowa; mobilność śmigłowcowa wojsk lądowych; zinformatyzowane systemy walki);
- utworzenie komitetu Rady Ministrów do spraw bezpieczeństwa narodowego (rządowego komitetu bezpieczeństwa narodowego) wraz z obsługującym go koncepcyjno-koordynacyjnym rządowym centrum bezpieczeństwa narodowego (RCBN – na bazie obecnego Rządowego Centrum Bezpieczeństwa);
- przyjęcie wieloletniego programu rozwoju (transformacji) systemu bezpieczeństwa narodowego (na bazie dotychczasowego programu pozamilitarnych przygotowań obronnych).

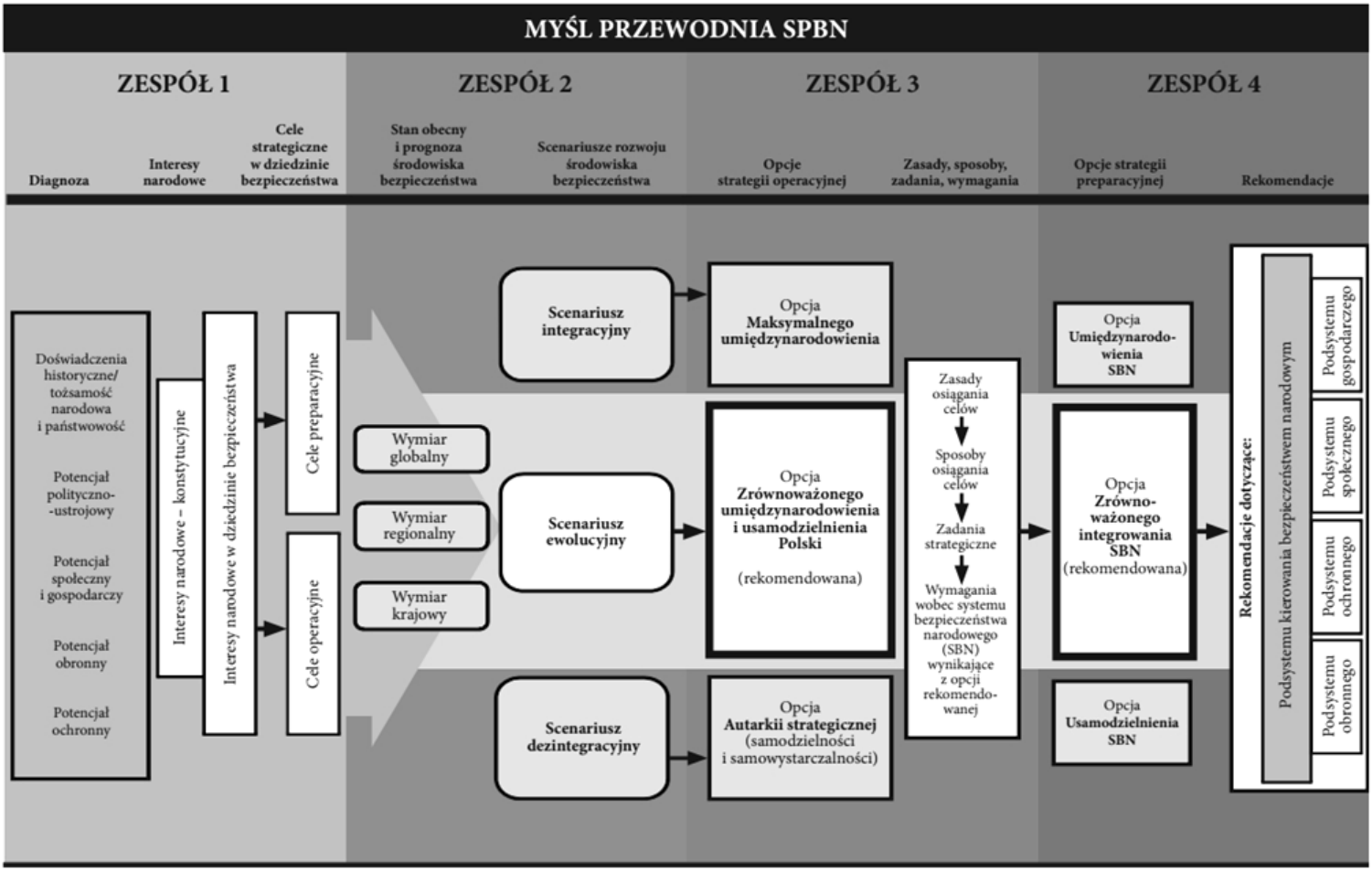
c) ewentualne zmiany konstytucyjne:

- wyeliminowanie niektórych zbyt szczegółowych, jak na ustawę zasadniczą, zapisów, nadając im charakter generalnych norm konstytucyjnych (za nadmiernie szczegółowe należałoby uznać np. literalne wymienianie konkretnych nazw instytucji, np. szef Sztabu Generalnego WP, dowódcy rodzajów Sił Zbrojnych);

- zrezygnowanie z odrębnej funkcji naczelnego dowódcy Sił Zbrojnych na czas wojny lub co najwyżej przewidzenie jej tylko fakultatywnie. W razie utrzymania tej funkcji jako konstytucyjnej – zapewnienie prawnej możliwości wskazania już w czasie pokoju osoby
  przewidzianej do jej objęcia na wypadek wojny;
- usunięcie niejasności konstytucyjnej co do podległości Sił Zbrojnych RP w czasie wojny ministrowi obrony narodowej;
- jednoznaczne, bezwarunkowe określenie organu kierującego obroną państwa w czasie wojny. Kompetencje w tym zakresie nie powinny być dzielone z innym organem (zasada
  jednolitości kierowania w warunkach wojny);
- gdyby miała być utrzymana właściwa dla czasu pokoju zasada współdziałania dwóch organów (Prezydenta i Rady Ministrów), w tym jednego kolektywnego, w kierowaniu obroną państwa – nadanie konstytucyjnie Radzie Gabinetowej kompetencji organu właściwego do zapewnienia tego współdziałania. W skład Rady Gabinetowej czasu wojny powinni dodatkowo być włączeni marszałkowie Sejmu i Senatu, jako potencjalni następcy Prezydenta;
- gdyby ewentualna nowelizacja Konstytucji RP zmierzała do zmiany obecnego modelu ustrojowego na prezydencki lub gabinetowy, należałoby:
  - w modelu prezydenckim – zmienić formułę Rady Bezpieczeństwa Narodowego z organu wyłącznie doradczego na konstytucyjny organ doradczo-koordynacyjny albo przekształcić w takowy Radę Gabinetową;
  - w modelu gabinetowym – w ogóle zrezygnować z konstytucyjnego usytuowania Rady Bezpieczeństwa Narodowego.

KATALOG INTERESÓW NARODOWYCH ORAZ CELÓW STRATEGICZNYCH W DZIEDZINIE BEZPIECZEŃSTWA

Interesy narodowe		**Cele strategiczne w dziedzinie bezpieczeństwa**	
Konstytucyjne (art. 5 Konstytucji RP)	**W dziedzinie bezpieczeństwa** (gotowość i zdolność zabezpieczenia interesów konstytucyjnych)	**Cele operacyjne (kierunki działań – gotowość)**	**Cele preparacyjne (zakres przygotowań – zdolności)**
Istnienie niepodległego, w nienaruszalnych granicach, państwa polskiego (państwo)	Dysponowanie skutecznym narodowym potencjałem bezpieczeństwa (gotowość i zdolność odstraszania, obrony i ochrony)	Prowadzenie aktywnej polityki wykorzystywania szans i uprzedzającego redukowania ryzyk w dziedzinie bezpieczeństwa	Budowa, utrzymanie i transformacja zintegrowanego systemu bezpieczeństwa narodowego, w tym podsystemu kierowania oraz podsystemów wykonawczych (operacyjnych i wsparcia)
		Utrzymywanie polityczno-decyzyjnej, planistycznej i szkoleniowej gotowości do skutecznego reagowania na zagrożenia dla niepodległości i nienaruszalności terytorialnej RP	
		Utrzymywanie ładu konstytucyjnego oraz wewnętrznej stabilności państwa	
	Członkostwo w wiarygodnych systemach bezpieczeństwa międzynarodowego	Udział w budowie i utrzymywaniu przez organizacje bezpieczeństwa, których Polska jest członkiem, operacyjnej gotowości do działania w wymiarach: polityczno-decyzyjnym, planistycznym i szkoleniowym	Wkład we wzmocnienie zdolności obronnych NATO oraz budowę zdolności obronnych UE
		Udział w międzynarodowych wysiłkach na rzecz redukowania źródeł zagrożeń,w tym w międzynarodowych operacjach bezpieczeństwa	Utrzymywanie narodowych zdolności do udziału w obronie sojuszników oraz operacjach ekspedycyjnych
Wolne i bezpieczne życie obywateli (obywatel i społeczeństwo)	Swoboda korzystania przez obywateli z praw i wolności człowieka, bez szkody dla bezpieczeństwa innych osób i bezpieczeństwa państwa	Udział w promowaniu na arenie międzynarodowej oraz krzewienie w społeczeństwie polskim zasad i świadomości należytego korzystania z praw i wolności człowieka i obywatela	Tworzenie i doskonalenie regulacji prawnych oraz edukacji powszechnej w zakresie praw i wolności
		Eliminowanie źródeł zagrożeń dla swobody korzystania z praw i wolności oraz konsekwentne ściganie i karanie sprawców wykroczeń przeciwko tej swobodzie	Organizowanie, wyposażanie oraz szkolenie służb i instytucji odpowiedzialnych za zapewnienie swobody korzystania z praw i wolności obywatelskich
	Ochrona indywidualna obywateli i zbiorowa ludności przed losowymi i celowymi zagrożeniami dla ich życia i zdrowia oraz przed naruszeniem, utratą lub degradacją dysponowanych przez nich dóbr (materialnych i niematerialnych)	Utrzymywanie wysokiej gotowości planistycznej, szkoleniowej i operacyjnej do szybkiego reagowania na zagrożenia kryzysowe (indywidualne dla obywateli i zbiorowe dla ludności oraz ich dóbr)	Doskonalenie regulacji prawnych w dziedzinie zarządzania kryzysowego, ochrony ludności i bezpieczeństwa publicznego
			Organizacyjno-techniczny rozwój (modernizacja) służb i instytucji odpowiedzialnych za ochronę ludności, bezpieczeństwo publiczne i zarządzanie kryzysowe
Rozwój społecznego potencjału państwa, z uwzględnieniem dziedzictwa narodowego (zasoby niematerialne)	Bezpieczne warunki rozwoju potencjału społecznego i gospodarczego RP / Społeczne i gospodarcze wsparcie bezpieczeństwa narodowego RP	Ochrona podmiotów (ogniw) potencjału społecznego i gospodarczego przed destrukcyjnym oddziaływaniem zewnętrznych i wewnętrznych zagrożeń w czasie pokoju, kryzysu i wojny / Informacyjne, edukacyjne, kulturowe, naukowo-techniczne, finansowe, energetyczne, infrastrukturalne, materiałowe i inne wsparcie działania operacyjnych ogniw systemu bezpieczeństwa narodowego	Doskonalenie zasad, procedur oraz zdolności współdziałania podmiotów (ogniw) społecznego i gospodarczego potencjału państwa ze służbami odpowiedzialnymi za ich ochronę i obronę w czasie pokoju, kryzysu i wojny / Opracowanie obowiązujących strategii, planów i programów przygotowania (utrzymania i doskonalenia) zdolności podmiotów (ogniw) społecznych i gospodarczych państwa do funkcjonowania w czasie zagrożenia (kryzysu) i wojny, w tym realizacji zadań wsparcia operacyjnych ogniw systemu bezpieczeństwa narodowego
Zrównoważony rozwój potencjału gospodarczego państwa, z uwzględnieniem m.in. ochrony środowiska naturalnego (zasoby materialne)			



UZASADNIENIE
DO PRZYGOTOWANEGO W BBN PROJEKTU USTAWY WPROWADZAJĄCEGO PROBLEMATYKĘ CYBERBEZPIECZEŃSTWA DO SYSTEMU AKTÓW PRAWNYCH

10 czerwca 2011 r. Prezydent RP Bronisław Komorowski przesłał do Sejmu RP projekt ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw.

Jego celem było stworzenie mechanizmów reagowania państwa na zagrożenia w cyberprzestrzeni, w tym ustawowe zdefiniowanie kategorii cyberprzestrzeni.

Przyjęta przez Parlament ustawa podpisana została przez Prezydenta RP 27 września 2011 r.

BIURO BEZPIECZEŃSTWA NARODOWEGO

10 czerwca 2011 r.

UZASADNIENIE DO PRZYGOTOWANEGO W BBN PROJEKTU USTAWY O ZMIANIE USTAWY O STANIE WOJENNYM ORAZ KOMPETENCJACH NACZELNEGO DOWÓDCY SIŁ ZBROJNYCH I ZASADACH JEGO PODLEGŁOŚCI KONSTYTUCYJNYM ORGANOM RZECZYPOSPOLITEJ POLSKIEJ ORAZ NIEKTÓRYCH INNYCH USTAW, WPROWADZAJĄCEJ PROBLEMATYKĘ CYBERBEZPIECZEŃSTWA DO SYSTEMU AKTÓW PRAWNYCH

Obecnie obserwuje się niezwykle dynamiczny proces przenoszenia aktywności ludzkiej w przestrzeń wirtualną, będącą składową obszaru cyberprzestrzeni. Dotyczy to nie tylko działalności osób fizycznych, ale również administracji publicznej, przedsiębiorców, organizacji społecznych i innych podmiotów. Działalność w cyberprzestrzeni staje się nieodzownym elementem funkcjonowania państwa i społeczeństwa. Należy jednak zauważyć, że postępujący proces informatyzacji, obok niewątpliwych korzyści, rodzi również określone zagrożenia. W szczególności dotyczy to możliwości wykorzystania cyberprzestrzeni w celach sprzecznych z interesami państwa i jego obywateli. Przykładem tego rodzaju zagrożeń są liczne ataki hakerów na różnego rodzaju instytucje o istotnym znaczeniu dla funkcjonowania państwa i społeczeństwa. Ataki takie mogą być niezwykle groźne, bowiem w ich efekcie może dojść do poważnych zakłóceń w funkcjonowaniu państwa, w tym jego struktur i gospodarki. Biorąc powyższe pod uwagę państwo powinno być przygotowane zarówno na odparcie takich ataków jak i zwalczanie jego skutków.

Zasadniczym celem zmian ujętych w projektowanej ustawie jest uwzględnienie zagrożeń wynikających z działań i zdarzeń w cyberprzestrzeni jako okoliczności spełniającej normatywną treść przesłanek wprowadzenia jednego ze stanów nadzwyczajnych, o których mowa w art. 229, 230 i 232 Konstytucji Rzeczypospolitej Polskiej.

Obowiązujące przepisy ustaw regulujących stany nadzwyczajne wskazują przyczyny wprowadzenia tych stanów, niemniej zostały one określone w sposób bardzo ogólnikowy. W związku z tym może to rodzić wątpliwości, co do ich charakteru i źródła.

Jest sprawą oczywistą, że niezbędną przesłanką wprowadzenia stanu nadzwyczajnego (o charakterze ogólnym) powinno stanowić zagrożenie dla określonego przez Konstytucję RP dobra (zewnętrzne zagrożenie państwa, zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego). Biorąc jednak pod uwagę ogromne zagrożenia związane z informatyzacją administracji publicznej i gospodarki narodowej, istnieje potrzeba jednoznacznego wskazania, że jedną z przyczyn wprowadzenia stanu nadzwyczajnego (o charakterze szczególnym) mogą być działania i zdarzenia w cyberprzestrzeni.

Uwzględniając powyższe, w projekcie przewiduje się dodanie w ustawie o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (art. 2 ust. 1) oraz w ustawie o stanie wyjątkowym (art. 2 ust. 1) wyrazów „*lub działaniami w cyberprzestrzeni*". W pierwszej z ww. ustaw proponuje się zdefiniowanie pojęcia „cyberprzestrzeni" która – zgodnie z projektem – oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

Ponadto w projekcie przewiduje się zastąpienie dotychczasowego terminu „*działania terrorystyczne"* sformułowaniem „*działania o charakterze terrorystycznymi*".

Niezależnie od powyższego w art. 3 w ust. 2 ustawy o stanie klęski żywiołowej przewiduje się, że katastrofę naturalną lub awarię techniczną mogą wywołać również zdarzenia w cyberprzestrzeni oraz działania o charakterze terrorystycznym.

Ponadto projekt przewiduje zmianę ustawy o stanie klęski żywiołowej (art. 3 ust. 2), gdzie zakłada się, że katastrofa naturalna lub awaria techniczna mogą zostać dodatkowo wywołane nie tylko przez działania terrorystyczne, ale również przez zdarzenia w cyberprzestrzeni.

W tym kontekście należy podkreślić, że rozporządzenia Prezydenta RP i Rady Ministrów o wprowadzeniu określonego stanu nadzwyczajnego mają charakter fakultatywny, a ich wydanie uzależnione jest zawsze od oceny stopnia zagrożenia w sferze zewnętrznego bądź wewnętrznego bezpieczeństwa państwa. Zatem ustawowe nadanie bezpieczeństwu w cyberprzestrzeni rangi istotnego segmentu bezpieczeństwa narodowego znajduje pełne uzasadnienie. W ten sposób bowiem wskazana ocena dokonywana będzie także przez pryzmat skutków naruszeń bezpieczeństwa w przestrzeni wirtualnej, dając w efekcie Prezydentowi RP i Radzie Ministrów poszerzony obraz skali występujących zagrożeń.

Ustawowe wyeksponowanie cyberprzestrzeni jako obszaru stwarzającego potencjalne zagrożenia, mogące skutkować koniecznością wprowadzenia jednego ze stanów nadzwyczajnych, nie ma charakteru precedensowego. Powiela ono bowiem rozwiązania przyjęte w toku prac parlamentarnych nad ustawami o stanach nadzwyczajnych, uznające – pod wpływem wydarzeń z dnia 11 września 2001 r. na terytorium USA – działania terrorystyczne za przyczynę powstania zagrożeń. Przedstawiony projekt pozostawia wskazaną przyczynę, dostosowując jedynie brzmienie formułujących ją zapisów do definicji przestępstwa o charakterze terrorystycznym, ujętej w art. 115 § 20 Kodeksu karnego.

Dodać należy, iż pojęcie cyberprzestrzeni nie jest obce obowiązującemu prawu. Operuje nim na przykład *Konwencja o cyberprzestępczości* z dnia 23 listopada 2001 r., implementowana do prawa polskiego ustawą z dnia 18 marca 2004 r. *o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń* (Dz. U. Nr 69, poz. 626), a także ratyfikowana *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji o współpracy w zwalczaniu terroryzmu, przestępczości zorganizowanej i innej przestępczości, podpisana w Ankarze w dniu 7 kwietnia 2003 r.* (Dz. U. z 2005 r. Nr 12, poz. 94).

Ujęte w projekcie rozwiązania wkomponowują się w przygotowywany przez Radę Ministrów „Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016", stanowiąc jego ważne uzupełnienie.

Wejście w życie projektowanej ustawy nie pociąga za sobą skutków finansowych dla budżetu państwa.

Projekt nie jest objęty zakresem prawa Unii Europejskiej.

RAPORT BBN:
ZASADY I PROCEDURY BEZPIECZEŃSTWA PRZEWOZU POWIETRZNEGO OSÓB ZAJMUJĄCYCH WAŻNE STANOWISKA PAŃSTWOWE

18 listopada 2010 r. Biuro Bezpieczeństwa Narodowego opublikowało raport dotyczący bezpieczeństwa lotów najważniejszych osób w państwie. Uwzględnione zostały w nim także ustalenia przyjęte na posiedzeniu Rady Bezpieczeństwa Narodowego 29 września 2010 r.

Tym samym zostało zrealizowane polecenie – wydane po katastrofie smoleńskiej przez wykonującego obowiązki Prezydenta marszałka Sejmu RP Bronisława Komorowskiego – opracowania procedur i przepisów dotyczących bezpieczeństwa lotów najważniejszych osób w państwie.

BIURO BEZPIECZEŃSTWA NARODOWEGO

18 listopada 2010 r.

RAPORT BBN: ZASADY I PROCEDURY BEZPIECZEŃSTWA PRZEWOZU POWIETRZNEGO OSÓB ZAJMUJĄCYCH WAŻNE STANOWISKA PAŃSTWOWE

SYNTEZA RAPORTU

Raport wychodzi z założenia, że bezpieczny transport lotniczy ważnych osób w państwie (VIP-ów) jest elementem szerszego problemu, jakim jest mobilność powietrzna strategicznego systemu kierowania państwem w warunkach pokoju, kryzysu i wojny. Zapewnienie jej wymaga w pierwszej kolejności zidentyfikowania ważnych (krytycznych) z punktu widzenia bezpieczeństwa narodowego kierowniczych stanowisk państwowych) i objęcie ich stosownymi rygorami bezpieczeństwa. Oprócz czterech konstytucyjnie najważniejszych osób funkcyjnych, których obecność na pokładzie nadaje statkowi powietrznemu status HEAD (Prezydent, marszałkowie Sejmu i Senatu, Premier), należą do nich także: ich zastępcy (wicemarszałkowie, wicepremierzy) kierownicy (ministrowie, szefowie) podległych im bezpośrednio podmiotów oraz kierownicy (prezesi, szefowie) innych krytycznych dla bezpiecznego funkcjonowania państwa organów konstytucyjnych (m.in. TK, TS, NIK, RPO, KRRiT, NBP, IPN, Prokurator Generalny), a także strategiczni dowódcy wojskowi (szef SGWP, dowódcy RSZ, DOSZ, SIWSZ), szefowie służb specjalnych (AW, ABW, CBA, SWW, SKW) i komendanci innych służb mundurowych (PP, SG, BOR, SP, SW, SC).

Z punktu widzenia bezpieczeństwa systemu kierowania państwem konieczne jest ustanowienie generalnych zasad takiego rozśrodkowania VIP-ów w czasie ich przemieszczania się, aby jednoczesna obecność na pokładzie statku powietrznego grupy tego typu osób nie powodowała przekroczenia poziomu racjonalnie dopuszczalnego ryzyka dla utrzymania gwarantowanej ciągłości kierowania podstawowymi funkcjami państwa. Oznacza to, że na pokładzie jednego statku powietrznego nie może znaleźć się więcej niż jedna z czterech najważniejszych osób w państwie oraz towarzyszyć jej może nie więcej niż 1/3 kierowników podległych jej bezpośrednio podmiotów oraz także nie więcej niż po 1/3 z grup kierowników pozostałych ważnych dla państwa instytucji (kierownicy podmiotów podległych innym najważniejszym osobom w państwie, pozostałe organy konstytucyjne, dowódcy wojskowi, szefowie i komendanci służb). Bezwzględnie obowiązywać musi zakaz lotu ze swoim pierwszym zastępcą, a w razie ich większej liczby z więcej niż połową zastępców. Konieczne jest określenie i następnie konsekwentne przestrzeganie w praktyce przez VIP-ów na pokładzie podstawowych wymagań bezpieczeństwa (terminowość, dyscyplina „pokładowa", zakaz wchodzenia do kokpitu w czasie startu i lądowania itp.).

Doprecyzowania wymagają obecne zasady i procedury organizacji powietrznego transportu VIP-ów. Spośród trzech podstawowych czynników determinujących realizację tych zadań – potrzeby (ambicje) polityczne, możliwości ekonomiczne (finansowe), wymagania

bezpieczeństwa – ten ostatni czynnik musi być traktowany jako stały; niedopuszczalne jest realizowanie ambicji politycznych lub szukanie oszczędności finansowych kosztem bezpieczeństwa („security first").

Konieczne jest doprecyzowanie odpowiedzialności koordynatora, poszczególnych organizatorów i wykonawców zadań transportu VIP-ów poprzez uzupełnienie obecnego porozumienia między nimi o wymienione w poprzednich akapitach zasady dotyczące VIP-ów, a także o dodatkowe sprawy koordynacji organizacyjnej i wykonawczej. Niezbędne jest zwłaszcza wprowadzenie dodatkowego obowiązku przeddecyzyjnej kontroli przygotowań operacji z punktu widzenia bezpieczeństwa i wyrażania ostatecznej zgody na jej przeprowadzenie. Kompetencję i odpowiedzialność taką powinien mieć koordynator, którym jest Kancelaria Prezesa Rady Ministrów, co oznacza konieczność utworzenia w niej specjalnej komórki bezpieczeństwa lotniczego VIP.

Uwaga: W związku z zastrzeżeniami KPRM wobec powyższego rozwiązania alternatywną opcją mogłoby być utworzenie takiej komórki w Rządowym Centrum Bezpieczeństwa – o ile podjęta byłaby jednocześnie decyzja o systemowej reformie kompetencyjnej, organizacyjnej i funkcjonalnej tej ponadresortowej instytucj – albo w Biurze Ochrony Rządu.

We wszystkich wariantach potrzebne jest wzmocnienie roli BOR w organizowaniu operacji. Nie może być ono pomijane, nie wystarczy tylko informowanie go, ani też wyłącznie konsultowanie przed ostatecznym zaplanowaniem misji.

Konieczne jest formalne usankcjonowanie i jednocześnie uregulowanie z odpowiednimi rygorami praktyki wykorzystywania przez najważniejsze osoby w państwie innych statków powietrznych niż celowo do tego dostosowane środki 36 splt (statki powietrzne innych rodzajów sił zbrojnych oraz lotnictwa służb publicznych – SG, PP). Przypadki takie muszą być ograniczone tylko do sytuacji nadzwyczajnej potrzeby (pilnej konieczności). Statki powietrzne spoza 36 splt powinny także mieć odpowiednie dopuszczenie do przewozu najważniejszych osób w państwie. W tym kontekście pilna staje się potrzeba przygotowania przez MON i MSWiA projektu ustawy o lotnictwie państwowym (z uwzględnieniem m.in. wprowadzenia prawnej ochrony dowódcy statku powietrznego przed presją i naciskami innych osób na pokładzie).

Odrębną sprawą wymagającą kompleksowej regulacji jest organizowanie przelotów VIP-ów przy wykorzystaniu lotnictwa cywilnego. Zakazane powinno być korzystanie przez czterech konstytucyjnych VIP-ów ze statków powietrznych prywatnego właściciela nie mającego statusu przewoźnika lotniczego. Szczegółowe warunki i zasady bezpieczeństwa w czasie korzystania z lotnictwa cywilnego powinny być ustalone formalnie w specjalnym porozumieniu między organizatorami (cztery kancelarie konstytucyjnych VIP-ów), BOR i Ministerstwem Infrastruktury oraz uwzględniane w negocjacjach z zamawianymi przewoźnikami. Zakres ustaleń powinien obejmować wszelkie możliwe formy lotów: rejsowe według rozkładu lotów, czartery długookresowe, czartery jednorazowe, a także loty okazjonalne, w tym przy wykorzystaniu śmigłowców. Szczególnie ważne jest zapewnienie we wszystkich przypadkach możliwości pełnego egzekwowania przez BOR ustalonych reguł bezpieczeństwa.

Podstawowym i głównym wykonawcą zadań transportu VIP-ów powinna pozostać formacja wojskowa (36 splt). Brak uzasadnienia dla przekazania ich wykonawcy cywilnemu. Wynika to z konieczności zapewnienia mobilności powietrznej i stabilności systemu kierowania państwem nie tylko w czasie pokoju, ale także w warunkach szczególnych zagrożeń (kryzysu i wojny). Konieczne są jednakże istotne zmiany w utrzymywaniu i funkcjonowaniu tego pułku. Dotyczyć one powinny doskonalenia w trzech podstawowych obszarach: organizacja lotów (uaktualnienie i poprawa procedur działania); przygotowanie kadr (dobór i szkolenie personelu); wyposażenie w potrzebny sprzęt (samoloty, trenażery, sprzęt wspomagający dowodzenie i szeroko rozumianą logistykę). Procedury realizacji zadań transportu VIP-ów przy pomocy lotnictwa specjalnego w warunkach pokojowych należy maksymalnie zbliżyć do procedur obowiązujących w lotnictwie cywilnym oraz zdecydowanie zwiększyć dyscyplinę organizacyjną i wykonawczą. Szczególne procedury, zbliżone do właściwych dla warunków kryzysowych i wojennych,

powinny być stosowane wyjątkowo tylko w przypadkach wystąpienia pilnej konieczności. W razie lotów na „niepewne" lotniska zawsze należy zadbać o szczegółowe dane o nich oraz poprzedzić lot rekonesansem w celu zredukowania ryzyka do racjonalnie dopuszczalnego poziomu (wysyłanie własnego kontrolera lotów, organizowanie dodatkowego podsystemu kierowania, korzystanie z opcji „lidera", wysyłanie własnych grup zabezpieczenia itp.)

Służba w 36 splt musi być najbardziej atrakcyjną służbą lotniczą w lotnictwie transportowym w Polsce. Oznacza to konieczność zwiększenia liczby pilotów w stosunku do liczby statków powietrznych, podwyższenia etatów wojskowych (w pułku powinni służyć piloci o długim stażu, a nie początkujący) oraz ustanowienia preferencyjnych warunków finansowych (specjalne dodatki rządowe do uposażenia, jako że jest to pułk realizujący głównie zadania ponadresortowe). Jednocześnie należy zwiększyć wymagania wobec personelu przez wymóg uzyskiwania i utrzymywania licencji cywilnych.

Zweryfikować system szkolenia pilotów, zwłaszcza ustanowić obowiązek szkolenia symulatorowego sytuacji awaryjnych w locie. Wprowadzić systematyczne gry i treningi z udziałem koordynatora, organizatorów i wykonawców zadań. Warto wreszcie rozważyć wniosek o szerszym, systemowym charakterze dotyczący ustanowienia i zorganizowania w Polsce zintegrowanego cywilno-wojskowego systemu szkolenia lotniczego.

Wykorzystać najbliższe lata na zakup i wprowadzenie na wyposażenie pułku 6 samolotów średniego zasięgu i 2 samolotów dużego zasięgu oraz śmigłowców, z bezwzględnym wyeliminowaniem obecnej, wyjątkowo niekorzystnej, różnorodności typów sprzętu. Dwa samoloty i dwa śmigłowce powinny być wyposażone jako powietrzne stanowiska (punkty) kierowania państwem, z uwzględnieniem wymagań sytuacji krytycznych (kryzysu i wojny).

Konieczna jest rozbudowa dotychczasowych zasad i procedur bezpieczeństwa podczas przewozu VIP-ów poprzez uzupełnienie ich o specjalne wymagania w razie wykonywania zadań w przypadkach szczególnych w czasie pokoju, ale także w nadzwyczajnych warunkach kryzysowych i wojennych. Oznacza to zwłaszcza bezwzględną konieczność dodatkowych czynności organizacyjnych i zabezpieczających (rekonesans, dodatkowa ochrona, dodatkowe środki łączności, środki ratownicze itp.) w razie lotu z VIP-em na nie w pełni przygotowane lotnisko lub w przewidywaniu trudnych warunków atmosferycznych, jak również dodatkową osłonę i obronę w razie wykonywania zadań w obliczu zagrożeń militarnych lub celowych zakłóceń elektronicznych. W warunkach wojennych najważniejsze osoby w państwie korzystać powinny przede wszystkim z Powietrznego Punktu Kierowania, czyli jednego ze specjalnie zawczasu przygotowanych do tego celu statków powietrznych 36 splt.

Na kanwie wniosków dotyczących bezpośrednio transportu powietrznego VIP-ów nasuwają się trzy dodatkowe wnioski o szerszym, systemowym charakterze. Pierwszy dotyczy propozycji uruchomienia prac nad programem budowy zintegrowanego, cywilno-wojskowego systemu funkcjonowania lotnictwa państwowego i cywilnego (zwłaszcza w zakresie szkolenia i infrastruktury lotniskowej). Drugi związany jest z koniecznością zapewnienia lotniska zapasowego dla VIP-ów w Warszawie, w kontekście mobilności powietrznej strategicznego systemu kierowania państwem, zwłaszcza w sytuacjach szczególnych (kryzysu i wojny). Trzeci wniosek mówi o zasadności rozważenia zorganizowania zintegrowanej, ponadresortowej komisji badania wypadków komunikacyjnych (nie tylko lotniczych).

Konkretne propozycje sposobu implementacji wniosków ujęte zostały w załączniku nr 8. Wdrażanie ich przez odpowiednie instytucje państwa powinno nastąpić po uprzednim ich rozpatrzeniu przez Radę Bezpieczeństwa Narodowego. Zadanie monitorowania realizacji wniosków i w razie potrzeby przedkładania raportów dla Rady Bezpieczeństwa Narodowego o stanie ich implementacji należałoby powierzyć Biuru Bezpieczeństwa Narodowego.

WSTĘP

Katastrofa smoleńska z jej dramatycznymi konsekwencjami postawiła na porządku dnia potrzebę przeanalizowania zasad i procedur zapewniania bezpieczeństwa transportu powietrznego osób zajmujących ważne (VIP), w tym najważniejsze (HEAD)[9], stanowiska państwowe. Jednocześnie zwróciła uwagę na istotny problem zapewnienia ciągłości funkcjonowania systemu kierowania państwem. Ważnym założeniem wyjściowym do podjęcia studiów nad tą problematyką musi bardziej ogólna konstatacja, że bezpieczny transport lotniczy VIP-ów jest elementem szerszego problemu, jakim jest **mobilność powietrzna strategicznego systemu kierowania państwem w warunkach pokoju, kryzysu i wojny**.

Na bazie wstępnych refleksji po katastrofie smoleńskiej można sformułować generalny problem, wymagający pogłębionej analizy studialnej, w formie następującego głównego pytania: **Jakie należałoby wprowadzić zmiany i uzupełnienia w obowiązujących zasadach i procedurach organizacji i realizacji zadań powietrznego przemieszczania się osób zajmujących ważne stanowiska państwowe, aby zwiększyć ich bezpieczeństwo i zminimalizować ryzyko występowania krytycznych sytuacji zagrażających ciągłości i sprawności funkcjonowania strategicznych ogniw systemu kierowania państwem?**

Dla rozwiązania tego problemu konieczne okazało się zbadanie trzech problemów szczegółowych:

1. Jakie zasady korzystania przez ważne osoby w państwie z transportu powietrznego należałoby ustanowić, a które z istniejących zmodyfikować, aby zwiększyć bezpieczeństwo realizacji zadań transportowych z wykorzystaniem statków powietrznych? Oznacza to konieczność analizy takich kwestii szczegółowych, jak ustalenie katalogu VIP-ów, podział ich na grupy z punktu widzenia znaczenia dla bezpieczeństwa państwa oraz kryterium ryzyka, sformułowanie fundamentalnych obowiązków ViP-ów w czasie korzystania z transportu lotniczego.
2. Jakie korekty należałoby wprowadzić do obowiązujących zasad i procedur organizacji powietrznego transportu VIP-ów, aby zapewniały optymalne i bezpieczne wykorzystanie państwowych i niepaństwowych statków powietrznych oraz jednoznaczność odpowiedzialności za poszczególne przedsięwzięcia organizacyjne? Oznacza to w szczególności rozpatrzenie takich kwestii, jak: podstawowe uwarunkowania mobilności powietrznej krytycznych ogniw systemu kierowania państwem; procedury organizowania transportu z wykorzystaniem lotnictwa państwowego; procedury organizowania transportu z wykorzystaniem lotnictwa cywilnego (niepaństwowego).
3. Jakie warunki muszą być spełnione, aby można było zapewnić bezpieczne wykonywanie zadań transportu powietrznego VIP-ów stosownie do potrzeb politycznego i strategicznego kierowania państwem? W ramach tego problemu konieczna jest szczegółowa analiza takich kwestii, jak: zasadność utrzymania obecnego rozwiązania, w którym za transport VIP-ów odpowiada przede wszystkim specjalna, do tego celu przeznaczona, jednostka wojskowa (36 splt); wymagania wobec przygotowania wojskowego lotnictwa specjalnego do realizacji zadań transportu VIP-ów (organizacyjne, kadrowe, szkoleniowe, sprzętowe); zasady bezpiecznego wykonywania zadań transportu powietrznego VIP-ów przez lotnictwo cywilne oraz w warunkach i przypadkach szczególnych.

Procedura analizy i rozwiązywania powyższych problemów obejmowała następujące przedsięwzięcia:

[9] Skrót VIP w niniejszym raporcie oznacza osoby zajmujące ważne (krytyczne z punktu widzenia bezpieczeństwa i ciągłości funkcjonowania państwa) stanowiska państwowe. W ramach tej kategorii osób wyróżnia się grupę czterech najważniejszych osób w państwie (tzw. konstytucyjnych VIP-ów lub HEAD-ów): Prezydent RP, marszałkowie Sejmu i Senatu oraz Prezes Rady Ministrów, których obecność na pokładzie statku powietrznego nadaje mu specjalny status HEAD. W skrótowej terminologii niniejszego Raportu: z punktu widzenia bezpieczeństwa systemu kierowania państwem VIP oznacza osoby funkcyjne ważne (krytyczne), HEAD – osoby najważniejsze (kluczowe).

1. Własne oceny i analizy BBN, w tym rozeznanie w rozwiązaniach w istniejących w innych krajach
2. Zebranie, analiza i ocena informacji i propozycji od innych instytucji państwowych
3. Wizyty studyjne w Dowództwie Sił Powietrznych oraz 36 splt
4. Narada z przedstawicielami cywilnych instytucji lotniczych
5. Trzy narady z przedstawicielami instytucji odpowiedzialnych za organizowanie, koordynowanie i zabezpieczanie transportu powietrznego VIP
6. Okrągły stół ekspertów lotniczych
7. Narada z cywilnymi dysponentami środków powietrznych oraz Ministerstwem Infrastruktury
8. Narada z Zarządem Krajowej Rady Lotnictwa
9. Indywidualne konsultacje z praktykami lotniczymi, ekspertami i niezależnymi analitykami zajmującymi się sprawami bezpieczeństwa i lotnictwa

Syntetyczne zestawienie kolejnych kroków procedury analitycznej przedstawia załącznik nr 1.

Całość problematyki niniejszego raportu ujęta została w trzech rozdziałach merytorycznych odpowiadających kolejno wymienionym wyżej trzem problemom szczegółowym. Ważniejsze kwestie przedstawione zostały dodatkowo w załącznikach 2–7.

Sposób implementacji zaproponowanych wniosków ujęto w załączniku nr 8.

Wszystkie materiały sporządzone, zebrane i wykorzystywane w ramach analizy studyjnej ujęte zostały w zbiorze (aneksie) dokumentów przechowywanym w Biurze Bezpieczeństwa Narodowego.

I. ZASADY KORZYSTANIA Z TRANSPORTU POWIETRZNEGO PRZEZ OSOBY ZAJMUJĄCE WAŻNE STANOWISKA PAŃSTWOWE

W niniejszym rozdziale przedstawione są rezultaty poszukiwania odpowiedzi na następujące pytanie: Jakie zasady korzystania przez ważne osoby w państwie z transportu powietrznego należałoby ustanowić, a które z istniejących zmodyfikować, aby zwiększyć bezpieczeństwo realizacji zadań transportowych z wykorzystaniem statków powietrznych? Obejmuje to analizę takich kwestii szczegółowych, jak ustalenie katalogu VIP-ów, podział ich na grupy z punktu widzenia znaczenia dla bezpieczeństwa państwa oraz kryterium ryzyka, sformułowanie fundamentalnych obowiązków ViP-ów w czasie korzystania z transportu lotniczego.

1. Katalog ważnych (krytycznych) stanowisk państwowych (VIP-ów)

Dotychczas obowiązująca w lotnictwie Sił Zbrojnych RP „Instrukcja organizacji lotów statków powietrznych o statusie HEAD" odnosi się tylko do czterech konstytucyjnych organów władzy: Prezydenta RP, marszałków Sejmu i Senatu oraz Prezesa Rady Ministrów. Ale nie ulega wątpliwości, że z punktu widzenia zapewnienia ciągłości funkcjonowania państwa nie jest to wystarczające. Dlatego w niniejszym Raporcie, choć wszystkie analizy i ustalenia dotyczą przede wszystkim owych czterech konstytucyjnych organów, uznaje się za zasadne odpowiednie poszerzenie rygorów bezpieczeństwa tak, aby objąć nimi także inne osoby funkcyjne reprezentujące ważne (krytyczne) funkcje państwa w sytuacjach, kiedy towarzyszą (mogą lub muszą towarzyszyć) konstytucyjnym VIP-om w lotach statkami powietrznymi. W związku z tym stosownymi rygorami procedur bezpieczeństwa należy objąć wszystkie podmioty uznane za ważne dla bezpiecznego funkcjonowania państwa (tzw. krytyczne ogniwa systemu kierowania państwem), a to oznacza w praktyce dodatkowe objęcie tymi rygorami[10]:

[10] Szczegółowy wykaz VIP-ów (Katalog VIP-ów) – zał. nr 2.

- zastępców głównych organów konstytucyjnych (konkretnie - wicemarszałków Sejmu i Senatu oraz wicepremierów);
- kierowników (ministrów, szefów) instytucji bezpośrednio podległych powyższym organom (członkowie Rady Ministrów, szefowie kancelarii obsługujących cztery najważniejsze organy władzy państwowej, szef BBN oraz dodatkowo – członkowie Rady Bezpieczeństwa Narodowego);
- kierowników (prezesów, przewodniczących, szefów) innych organów ważnych (krytycznych) dla bezpiecznego funkcjonowania państwa – w tym ustanowionych bezpośrednio przez Konstytucję (TK, TS, NIK, RPO, KRRiT, NBP, IPN, Prokurator Generalny) oraz strategicznych dowódców wojskowych (szef SGWP, dowódcy RSZ, DOSZ, SIWSZ), szefów służb specjalnych (AW, ABW, CBA, SWW, SKW), a także komendantów innych służb mundurowych (PP, SG, BOR, SP, SW, SC).

2. Kryteria rozśrodkowania VIP-ów na potrzeby transportu powietrznego

Przyjmując za kryterium zapewnienie bezpieczeństwa systemu kierowania państwem, a w tym konieczność redukowania ryzyka związanego z wykorzystaniem w tym systemie środków transportu powietrznego, należy ustanowić w miarę uniwersalny model takiego organizacyjnego rozśrodkowania VIP-ów, aby jednoczesna obecność na pokładzie tego samego statku powietrznego grupy tego typu osób (istotnych dla systemu kierowania państwem) nie powodowała przekroczenia poziomu racjonalnie dopuszczalnego ryzyka dla utrzymania gwarantowanej ciągłości kierowania podstawowymi funkcjami państwa. Z analizy rozwiązań stosowanych w innych państwach wynika, że problem ten jest różnie rozstrzygany: rzadko przy pomocy konkretnych regulacji prawnych, częściej na zasadzie mniej lub bardziej sformalizowanych zaleceń lub po prostu „utartej praktyki".

Również u nas nie wydaje się konieczne wprowadzanie rygorystycznych przepisów prawnych regulujących tę problematykę. Potrzebne jest jednak i jednocześnie powinno wystarczyć opracowanie i sformułowanie w postaci zaleceń lub wytycznych ujętych w odpowiednich dokumentach doktrynalnych z dziedziny bezpieczeństwa narodowego (np. w Polityczno-Strategicznej Dyrektywie Obronnej, Planie Zarządzania Kryzysowego) ogólnych zasad rozśrodkowania podstawowych (krytycznych) elementów tego systemu w czasie transportu powietrznego. Zasadami tymi powinni każdorazowo kierować się organizatorzy lotów VIP-ów, którzy powinni te zasady dodatkowo skonkretyzować (rozwinąć) w swoich wewnętrznych dokumentach organizacyjnych (statutach, regulaminach, instrukcjach, wytycznych itp.).

Pomocne w sformułowaniu i realizacji zasady rozśrodkowania VIP-ów może być posłużenie się analogią do metody tzw. „koszyków" stosowanej przy rozstawianiu drużyn piłkarskich podczas ustalania grup eliminacyjnych do dużych turniejów (mistrzostwa świata lub Europy). Przyporządkowanie osób zajmujących krytyczne stanowiska w systemie kierowania państwem do określonych grup („koszyków") byłoby instrumentem wykluczającym „spotkanie" się dwóch lub więcej najważniejszych (konstytucyjnych) VIP-ów na pokładzie jednego statku powietrznego, a także spotkanie się tam nadmiernej liczby innych osób funkcyjnych o podobnej randze i podobnym znaczeniu dla ciągłości funkcjonowania państwa.

Proponujemy następujące trzy „koszyki" VIP-ów[11]:

- A: Prezydent RP, marszałkowie Sejmu i Senatu, Prezes Rady Ministrów oraz
- „podkoszyk A.1" – ich zastępcy (konkretnie – wicemarszałkowie i wicepremierzy);
- B: kierownicy (szefowie) podmiotów bezpośrednio podległych powyższym organom (ministrowie, szefowie kancelarii obsługujących cztery najważniejsze organy władzy państwowej, szef BBN, członkowie RBN) oraz
- „podkoszyk B.1" – ich zastępcy (wiceministrowie);

[11] Załącznik nr 3.

- C: kierownicy (prezesi, szefowie) innych podmiotów ważnych (krytycznych) dla bezpiecznego funkcjonowania państwa – w tym ustanowionych bezpośrednio przez Konstytucję (TK, TS, NIK, RPO, KRRiT, NBP, IPN, także Prokurator Generalny) oraz strategiczni dowódcy wojskowi (szef SGWP, dowódcy RSZ, DOSZ, SIWSZ), szefowie służb specjalnych (AW, ABW, CBA, SWW, SKW), a także komendanci służb mundurowych (PP, SG, BOR, SP, SW, SC) oraz
- „podkoszyk C.1" – ich zastępcy (wiceprezesi, wiceprzewodniczący).

W trakcie ustalania grupy (składu delegacji) VIP-ów należy tak korzystać z owych „koszyków", aby przestrzegać następujących zasad:

1) na pokładzie tego samego statku powietrznego nie może przebywać w czasie jednego lotu więcej niż jedna osoba spośród najważniejszych osób w państwie;
2) najważniejsza osoba w państwie nie może podróżować ze swoim zastępcą, a w razie większej liczby zastępców, na pokładzie nie może się znaleźć więcej niż ich połowa;
3) z najważniejszą osobą w państwie nie może podróżować więcej niż 1/3 podległych jej lub innej osobie spośród najważniejszych osób w państwie kierowników jednostek organizacyjnych (instytucji państwa);
4) najważniejszej osobie w państwie może towarzyszyć nie więcej niż 1/3 innych ważnych dla bezpiecznego funkcjonowania państwa kierowników instytucji państwa, ujętych w wykazie tzw. krytycznych stanowisk w systemie kierowania bezpieczeństwem narodowym, ustalonym w odrębnym trybie.

3. Obowiązki VIP-a na pokładzie

Istnieje niewątpliwie potrzeba jednoznacznego zdefiniowania, uświadomienia i konsekwentnego egzekwowania bardziej rygorystycznego przestrzegania przez VIP-ów wszystkich wymagań bezpieczeństwa w czasie przelotu. W katalogu takich wymagań[12] należy podkreślić szczególnie:

- Konieczność rygorystycznego przestrzegania terminowości realizacji zaplanowanych przedsięwzięć. Każda zmiana w ostatniej chwili listy pasażerów lub czasu startu wprowadza dodatkowe ryzyko, a także wiąże się z dodatkowymi kosztami i obciążeniami załóg lotniczych;
- Na pokładzie statku powietrznego jedynym dowódcą jest dowódca załogi. VIP nie ma prawa wydawania mu jakichkolwiek poleceń, a ma obowiązek wykonywania wszelkich poleceń dowódcy statku powietrznego;
- Obowiązuje zakaz wchodzenia do kabiny pilotów w newralgicznych fazach lotu (w czasie startu i lądowania). Drzwi do kabiny pilotów powinny być wtedy zamknięte;
- Każdy VIP na pokładzie musi podporządkować się ogólnym przepisom (np. stosowne zakazy korzystania ze środków elektronicznych) oraz poleceniom służb bezpieczeństwa.

Wskazane byłoby ujęcie tej problematyki w ramach dokumentów organizacyjnych, administracyjnych i porządkowych podpisywanych przez każdą osobę funkcyjną w czasie obejmowania stanowiska (podobnie jak to jest w przypadku przyjmowania do wiadomości regulacji dotyczących np. ochrony tajemnicy lub BHP).

* * *

Wdrożenie tych zaleceń powinno być zapewnione przez ujęcie ich w porozumieniach między organizatorami i wykonawcami zadań transportu VIP-ów. Każda instytucja z katalogu ogniw krytycznych w systemie kierowania państwem powinna we własnych regulacjach wewnętrznych (statuty, regulaminy, instrukcje itp.) ustalić zasady wspólnego podróżowania

[12] Załącznik nr 4.

transportem powietrznym osób kierowniczych. Problematyka ta powinna także znaleźć swoje odzwierciedlenie w Polityczno-Strategicznej Dyrektywie Obronnej i Krajowym Planie Zarządzania Kryzysowego oraz przeniesiona odpowiednio do operacyjnych dokumentów (planów) wykonawczych tych instytucji centralnych, które zakwalifikowane zostały do grupy krytycznych ogniw systemu kierowania państwem.

II. ORGANIZOWANIE TRANSPORTU POWIETRZNEGO OSÓB ZAJMUJĄCYCH WAŻNE STANOWISKA PAŃSTWOWE

Treścią niniejszego rozdziału jest poszukiwanie odpowiedzi na pytanie: Jakie korekty należałoby wprowadzić do obowiązujących zasad i procedur organizacji powietrznego transportu VIP-ów, aby zapewniały optymalne i bezpieczne wykorzystanie państwowych i niepaństwowych statków powietrznych oraz jednoznaczność odpowiedzialności za poszczególne przedsięwzięcia organizacyjne? Oznacza to w szczególności rozpatrzenie takich kwestii, jak: podstawowe uwarunkowania mobilności powietrznej krytycznych ogniw systemu kierowania państwem; procedury organizowania transportu z wykorzystaniem lotnictwa państwowego; procedury organizowania transportu z wykorzystaniem lotnictwa cywilnego (niepaństwowego).

1. Podstawowe uwarunkowania mobilności powietrznej krytycznych ogniw systemu kierowania państwem

Rozważając tę problematykę warto zauważyć, że w dużej mierze można ją sprowadzić do dylematu uzyskania stosownego balansu między trzema czynnikami[13]:

- ambicje polityczne - czyli, oczekiwania i potrzeby sprawnego, skutecznego, szybkiego i elastycznego funkcjonowania państwa, w tym władz państwowych, szczególnie na arenie międzynarodowej, ale także w kraju. Im większa mobilność i swoboda przemieszczania się organów władzy i administracji publicznej (transport powietrzny daje największe w tym zakresie możliwości), tym można formułować i osiągać ambitniejsze cele oraz realizować ambitniejsze programy polityczne;
- koszty ekonomiczne, w tym finansowe – czyli uwarunkowania, możliwości i ograniczenia w dysponowaniu odpowiednimi zasobami finansowymi, sprzętem lotniczym, należycie przygotowanymi kadrami oraz możliwościami realizacji wszelkich przedsięwzięć zabezpieczających;
- rygory bezpieczeństwa – czyli kryteria i wymagania formułowane z punktu widzenia potrzeb bezpieczeństwa wobec zasobów kadrowych i sprzętowych oraz procedur organizacyjnych i wykonawczych podczas realizacji zadań transportu powietrznego VIP-ów.

Należy jednoznacznie stwierdzić, że w poszukiwaniu balansu między tymi trzema czynnikami **swoboda manewru decyzyjnego istnieje tylko między ambicjami politycznymi i kosztami ekonomicznymi. Rygory bezpieczeństwa muszą być constans. Nie można za cenę bezpieczeństwa maksymalizować ambicji, ani też minimalizować kosztów ekonomicznych (oszczędzać na bezpieczeństwie)**.

Oznacza to, że wraz ze wzrostem naszych ambicji politycznych, a są one naturalnym następstwem choćby naszego członkostwa w NATO i UE, muszą rosnąć także nakłady na konieczne środki do realizacji zadań mobilności powietrznej podstawowych organów władzy i administracji publicznej. Należy to obowiązkowo uwzględnić w ustalaniu budżetu MON, a być może najwłaściwszym rozwiązaniem byłoby ustanowienie oddzielnej pozycji w budżecie państwa na ten cel.

[13] Załącznik nr 5.

2. Organizowanie transportu z wykorzystaniem lotnictwa państwowego (lotnictwa wojskowego i lotnictwa służb publicznych)

Podstawowymi dokumentami regulującymi obecnie zasady i procedury planowania i koordynowania zadań transportu powietrznego najważniejszych osób w państwie są: *decyzja nr 359/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 roku w sprawie trybu wykorzystania wojskowych transportowych statków powietrznych na potrzeby Sił Zbrojnych; Porozumienie w sprawie wojskowego specjalnego transportu lotniczego zawarte 15 grudnia 2004 roku pomiędzy kancelariami Prezydenta RP, Sejmu, Senatu, Prezesa Rady Ministrów i Ministrem Obrony Narodowej, Instrukcja organizacji lotów statków powietrznych o statusie HEAD (wprowadzona decyzją MON nr 184 z 9.06.2009); Porozumienie zawarte w dniu 18 marca 2008 roku pomiędzy Biurem Ochrony Rządu a Siłami Powietrznymi,* określajace zasady współpracy podczas organizacji i wykonywania zadań lotniczych z osobami uprawnionymi do korzystania z ochrony BOR.

Generalnie ocenia się, że regulacje zawarte w przywołanych dokumentach są prawidłowe. Wymagają jednakże uzupełnienia w co najmniej trzech istotnych obszarach, które powinny być uwzględnione w nowym (znowelizowanym) porozumieniu między koordynatorem, organizatorami i wykonawcami zadań transportu powietrznego VIP-ów[14]:

- Pierwszy – to doprecyzowanie odpowiedzialności poszczególnych organizatorów i wykonawców w ramach ich współdziałania, a zwłaszcza ustanowienie jednoznacznych kompetencji i obowiązków koordynatora, którym jest Kancelaria Prezesa Rady Ministrów. Do jej zadań dotychczasowych, ograniczających się w zasadzie do koordynacji dysponowania limitem, należy dodać m.in. zadanie ostatecznej kontroli przygotowań (organizacji) każdej operacji o statusie HEAD z punktu widzenia bezpieczeństwa (wg tzw. „check-listy", czyli listy sprawdzeń lub potwierdzeń, obejmującej m.in sprawdzenie przestrzegania ustalonych zasad rozśrodkowania VIP-ów, potwierdzenie stanu lotniska docelowego, obowiązkowego wyznaczania i zabezpieczenia lotnisk zapasowych – do tej pory takie potwierdzenia realizuje się tylko incydentalnie: wizyty Papieża lub prezydenta USA). Wymaga to utworzenia w KPRM specjalnej, kompetentnej komórki bezpieczeństwa lotniczego. Ponieważ szef Kancelarii Prezesa Rady Ministrów zgłasza zastrzeżenia co do tego kompetencyjnie i organizacyjnie optymalnego w dzisiejszych realiach rozwiązania, to w razie uwzględnienia tych zastrzeżeń alternatywną opcją mogłoby być utworzenie takiej komórki w Rządowym Centrum Bezpieczeństwa – o ile podjęta byłaby jednocześnie decyzja o (rzeczywiście koniecznej z innych, bardziej generalnych powodów) systemowej reformie kompetencyjnej, organizacyjnej i funkcjonalnej tej ponadresortowej instytucji. Jeszcze innym, ale systemowo wyraźnie najsłabszym rozwiązaniem mogłoby być powierzenie takiego zadania Biuru Ochrony Rządu i tym samym utworzenie w BOR dodatkowej komórki bezpieczeństwa lotniczego VIP.[15] Niezależnie od swej lokalizacji nowa komórka bezpieczeństwa lotniczego VIP winna ostatecznie wyrażać zgodę na realizację danego przedsięwzięcia (w szczególnych sytuacjach poprzedzoną przeprowadzeniem gry decyzyjnej dla sprawdzenia jakości przygotowania operacji). W realizacji swoich zadań powinna ona stosować procedury zarządzania ryzykiem (wyprzedzające oceny zagrożeń w ramach planowania operacji i oceny poziomu ryzyka w stosunku do ryzyka akceptowalnego);
- Drugi – to ustalenie i zapewnienie sprawnego współdziałania między koordynatorem (KPRM), organizatorem (konkretna w danym przypadku kancelaria VIP-a o statusie HEAD)

[14] Projekt nowego, poszerzonego porozumienia między kancelariami Prezydenta, Sejmu, Senatu i Prezesa Rady Ministrów oraz MON i MSWiA – zał. nr 6.

[15] Propozycja KPRM, zgłoszona jako alternatywna dla proponowanego przyjęcia przez nią tych zadań, aby kontrolę przygotowań wylotu powierzyć Siłom Powietrznym i BOR w ramach ich właściwości, nie może być uwzględniona. Wówczas bowiem wykonawcy zadania w sferze lotniczej i w sferze bezpieczeństwa sami kontrolowaliby swoje czynności. Praktycznie więc nie byłoby nad nimi żadnej kontroli – czyli sytuacja pozostałaby taką, jaką jest obecnie: bez systemowej koordynacji i nadzoru.

i wykonawcą zadań lotniczych (państwowym lub cywilnym), a BOR odpowiedzialnym za bezpieczeństwo najważniejszych osób w państwie. Konieczne jest wzmocnienie roli BOR w organizowaniu operacji. Nie może być ono pomijane, nie wystarczy tylko informowanie go, ani też wyłącznie konsultowanie przed ostatecznym zaplanowaniem misji. Wymagania bezpieczeństwa formułowane przez BOR powinny być usankcjonowane w stosownym porozumieniu między koordynatorem, organizatorami i wykonawcami lotów z najważniejszymi osobami w państwie;

- Trzeci – formalne usankcjonowanie i jednocześnie uregulowanie z odpowiednimi rygorami praktyki wykorzystywania przez najważniejsze osoby w państwie (HEAD) innych niż należące do 36 splt (i mające odpowiednie dopuszczenia do tego rodzaju lotów) statków powietrznych lotnictwa państwowego. Idzie tu np. o statki powietrzne należące do innych formacji Sił Powietrznych oraz pozostałych rodzajów Sił Zbrojnych (Wojska Lądowe, Marynarka Wojenna), a także statki powietrzne lotnictwa służb publicznych (Straży Granicznej i Policji Państwowej). Wykorzystywanie tego typu środków przez najważniejsze osoby w państwie powinno być ograniczone tylko i wyłącznie do sytuacji nadzwyczajnej potrzeby (pilnej konieczności) – gdy istnieje nagła, niespodziewana i ważna konieczność lotu, a żaden ze środków 36 splt nie jest dostępny w potrzebnym czasie. Należy jednak wprowadzić zasadę i zapewnić jej rygorystyczne przestrzeganie, że także spośród pozostałych (poza 36 splt) statków powietrznych lotnictwa wojskowego oraz lotnictwa służb publicznych do przewozu najważniejszych osób w państwie mogą być wykorzystywane tylko te, które wcześniej uzyskają stosowne dopuszczenia do ewentualnej realizacji tego typu zadań o statusie HEAD. Takich dopuszczeń (certyfikatów) udzielać powinny odpowiednio MON i MSWiA. W tym kontekście należałoby także rozważyć opracowanie ustawy o lotnictwie państwowym (MON i MSWiA). W ramach nowych regulacji ustawowych zasadne wydaje się m.in. wprowadzenie ochrony prawnej dowódcy załogi przed naciskami i presją innych osób będących na pokładzie statku powietrznego.

3. Organizowanie transportu w razie korzystania z lotnictwa cywilnego (niepaństwowego)

VIP-y coraz częściej korzystają z przelotów samolotami cywilnymi, w tym czarterowanymi lub rejsowymi, a nawet prywatnymi statkami powietrznymi. Tymczasem brak jest procedur regulujących postępowanie w tym względzie w podobny sposób, jak to jest w stosunku do lotów z wykorzystaniem państwowych specjalnych statków powietrznych. Ten brak generuje ryzyko zagrożeń dla samych VIP-ów oraz powoduje perturbacje w podróżowaniu pozostałych osób. Istnieje zatem niewątpliwie pilna konieczność opracowania zasad i procedur organizacji i zabezpieczenia przewozu VIP-ów cywilnymi statkami powietrznymi. Dotyczy to w szczególności czterech najważniejszych osób w państwie (HEAD), a w przypadku lotów czarterowych – odpowiednio także innych VIP-ów (w podobnym zakresie jak w przypadku lotnictwa państwowego).

W zestawie takich zasad należałoby ująć przede wszystkim określone przez BOR jednoznaczne wymagania i procedury, od których spełnienia zależy możliwość korzystania przez HEAD-ów z cywilnych (niepaństwowych) środków transportu powietrznego. Dotyczyć one mogłyby np. zasady preferowania lotów czarterowych przed rejsowymi; wymagań wobec pilotów, tj. ich doświadczenia zawodowego; rodzaju samolotów i śmigłowców oraz ich dodatkowego wyposażenia; sposobów finansowania dodatkowych przedsięwzięć związanych z bezpieczeństwem VIP-ów w czasie takiego lotu itp. W przypadku lotów czarterowanych należy również wprowadzić zasadę sprawdzania przez BOR niepaństwowych statków powietrznych oraz ich ochrony po wykonanym oblocie komisyjnym na lotniskach i lądowiskach, a także zakaz korzystania przez VIP-ów kategorii HEAD z prywatnych statków powietrznych należących do właściciela, który nie jest przewoźnikiem lotniczym.

W sumie szczegółowe warunki i zasady korzystania z lotnictwa cywilnego z uwzględnieniem wymagań i rygorów bezpieczeństwa powinny być ustalone formalnie w specjalnym porozumieniu między koordynatorem, organizatorami, Ministerstwem Infrastruktury i BOR

oraz uwzględniane przez organizatorów lotów w negocjacjach z odpowiednimi podmiotami (przewoźnikami) cywilnymi. Zakres ustaleń powinien obejmować wszelkie możliwe formy lotów: rejsowe według rozkładu lotów, czartery długookresowe, czartery jednorazowe, a także loty okazjonalne, w tym przy wykorzystaniu śmigłowców[16]. Szczególnie ważne jest zapewnienie we wszystkich przypadkach możliwości pełnego egzekwowania przez BOR ustalonych reguł bezpieczeństwa.

* * *

Wdrożenie tych zaleceń powinno nastąpić poprzez ujęcie ich w dwóch porozumieniach: a) znowelizowanym porozumieniu między kancelariami konstytucyjnych VIP-ów oraz MON i MSWiA – w odniesieniu do lotnictwa państwowego; b) w nowym porozumieniu między tymiż kancelariami oraz Ministerstwem Infrastruktury i BOR – w odniesieniu do lotnictwa cywilnego.

III. WYKONYWANIE ZADAŃ TRANSPORTU POWIETRZNEGO OSÓB ZAJMUJĄCYCH WAŻNE STANOWISKA PAŃSTWOWE

Treścią niniejszego rozdziału jest poszukiwanie odpowiedzi na pytanie: Jakie warunki muszą być spełnione, aby można było zapewnić bezpieczne wykonywanie zadań transportu powietrznego VIP-ów stosownie do potrzeb politycznego i strategicznego kierowania państwem? W ramach tego problemu konieczna jest szczegółowa analiza takich kwestii, jak: zasadność utrzymania obecnego rozwiązania, w którym za transport VIP-ów odpowiada przede wszystkim specjalna, do tego celu przeznaczona, jednostka wojskowa (36 splt); wymagania wobec przygotowania wojskowego lotnictwa specjalnego do realizacji zadań transportu VIP-ów (organizacyjne, kadrowe, szkoleniowe, sprzętowe); zasady bezpiecznego wykonywania zadań transportu powietrznego VIP-ów przez lotnictwo cywilne oraz w warunkach i przypadkach szczególnych.

1. Państwowy główny wykonawca zadań transportu powietrznego VIP-ów

Pierwszy problem, jaki należy rozstrzygnąć, to określenie rodzaju podmiotu odpowiedzialnego za transport powietrzny VIP-ów: czy to ma być nadal specjalna jednostka wojskowa, czy może podmiot cywilny? Przeprowadzone analizy zdecydowanie wykazują, że powinna to nadal być jednostka wojskowa. W zasadzie wszystkie konsultowane instytucje i zdecydowana większość ekspertów opowiada się za takim wariantem.

Przyjmując takie rozwiązanie należy zatem pozostawić 36 splt. Wynika to z konieczności zapewnienia potrzebnej na co dzień, ale przede wszystkim nieodzownej w sytuacjach szczególnych zagrożeń (w razie kryzysu i wojny), mobilności powietrznej i stabilności systemu kierowania państwem. Wnioski z katastrofy smoleńskiej, ale także szersze analizy wskazują jednakże na konieczność istotnych zmian w zasadach, warunkach i sposobach utrzymywania oraz wykorzystywania tego pułku zgodnie z jego podstawowym przeznaczeniem.

Przede wszystkim zasadne wydaje się rozważenie wprowadzenia wymogu certyfikacji 36 splt oraz wprowadzenie obowiązku uzyskiwania licencji cywilnych dla pilotów tego pułku wraz z wymogiem systematycznego szkolenia i weryfikacji na symulatorach lotu klasy D.

Powinno się wykorzystać okres czarterowania EMBRAERÓW na wdrożenie zaleceń organizacyjno-technicznych i sprawnościowych (operacyjnych) oraz przygotowanie 36 splt do realizacji zadań bezpiecznego transportu VIP-ów w warunkach pokoju, kryzysu i wojny.

Równolegle z utrzymywaniem pułku specjalnego w szerszym zakresie należałoby odpowiednio przygotowywać do realizacji zadań na rzecz mobilności powietrznej systemu kierowania

[16] Projekt porozumienia w sprawie bezpieczeństwa lotów statkami powietrznymi lotnictwa cywilnego z najważniejszymi osobami w państwie – zał. nr 7.

państwem, zwłaszcza w sytuacjach szczególnych, także inne zasoby transportu powietrznego w Polsce: pozostałe lotnictwo wojskowe, lotnictwo służb publicznych oraz – np. w ramach programów przygotowań obronnych – lotnictwo cywilne (firmy komercyjne, prywatnych właścicieli).

2. Przygotowanie specjalnego lotnictwa wojskowego (36 splt) do realizacji zadań transportu VIP-ów

Dla zapewnienia potrzebnych warunków skutecznej realizacji zadań przez 36 splt konieczne jest wprowadzenie szeregu zmian do dotychczasowej praktyki jego utrzymywania i funkcjonowania. Do najważniejszych i najpilniejszych należy zaliczyć:

- *W sferze organizacyjno-operacyjnej (procedury przygotowywania i wykonywania zadań)*
  - Zmodyfikować procedury wykonywania lotów z VIP-ami zbliżając je do procedur cywilnych lub po prostu wdrażając w pełni procedury cywilne;
  - Zwiększyć dyscyplinę organizacyjną i wykonawczą (rygorystyczne przestrzeganie terminów i przepisów instrukcyjnych dotyczących przygotowania i wykonania lotów);
  - Rozważyć wprowadzenie wymagania, aby pułk posiadał Certyfikat Przewoźnika Lotniczego (tzw. AOC) zgodny z europejskim prawem lotniczym;
  - W razie lotów na „niepewne" lotniska – zawsze poprzedzać je uzyskaniem szczegółowych danych o nim oraz rekonesansem i konsekwentnie realizować przedsięwzięcia wymagane tzw. listą potwierdzeń. Obejmować one powinny m.in. sprawdzanie przed przylotem VIP-ów, czy dane lotnisko rzeczywiście spełnia podane wcześniej parametry bezpieczeństwa, a w razie jakichkolwiek zastrzeżeń dokonać wnikliwej oceny ryzyka, jakie stwarzają one dla lądowania tam najważniejszych osób w państwie i następnie wprowadzanie procedur redukowania tego ryzyka: np. obowiązkowo wysyłać kontrolera lotów (wieżowego) i organizować podsystem kierowania samolotem od startu do lądowania, a ponadto korzystać z opcji „lidera", kierowania własnych grup zabezpieczenia na lotnisko, stosować zwiększone wymagania wobec pilotów wyznaczonych do danego zadania itp.;
  - Przeanalizować, zweryfikować i dokonać syntezy ocen przyczyn dotychczasowych wypadków i katastrof w lotnictwie wojskowym korzystając z zasad obowiązujących w lotnictwie cywilnym (*Zasada dobrych praktyk*) i udoskonalić system wykorzystywania wniosków z tych analiz.

- *W sferze kadrowej i szkoleniowej*:
  - Służba w 36 splt musi być najbardziej atrakcyjną służba lotniczą w ramach lotnictwa transportowego w Polsce (nie tylko wśród pilotów wojskowych, ale powinna być atrakcyjna także dla pilotów cywilnych). Oznacza to przede wszystkim zapewnienie możliwości rozwoju i awansu zawodowego (wyższe etaty wojskowe, niejako wymuszające służbę w 36 splt doświadczonych, o dłuższym stażu pilotów lotnictwa transportowego) oraz wprowadzenie preferencyjnych warunków finansowych (specjalne **dodatki rządowe** do uposażenia), które zapewniałyby możliwość selekcji najlepszych do tej służby na podstawie naturalnej konkurencji wśród wszystkich zainteresowanych tym pilotów w Polsce: zarówno wojskowych, jak i cywilnych (na specjalnych kontraktach). To nie może być tylko zwykłe kierowanie tam do służby chętnych;
  - Zapewnić lepszą niż w innych jednostkach lotniczych proporcję liczby pilotów w stosunku do sprzętu (wymagają tego względy szczególnej stałej

dyspozycyjności oraz specyfiki realizacji zadań już w warunkach pokojowych – np. niepewność czasowa rozpoczęcia zadania);
- Zweryfikować system szkolenia pilotów. Wprowadzić konieczność uzyskiwania i potwierdzania przez pilotów i techników licencji cywilnych z odpowiednimi uprawnieniami. Rozważyć zawarcie umowy z przewoźnikami cywilnymi w sprawie lotów pilotów 36 splt w cywilnych liniach lotniczych (powrócić do takowej praktyki sprzed lat);
- Wprowadzić systematyczne treningi na symulatorach, zwłaszcza z uwzględnieniem sytuacji awaryjnych. Bezwzględnie przestrzegać zasady wykorzystywania symulatorów o parametrach technicznych odpowiadajacych typom sprzętu uzytkowanego w 36 splt (konieczność uniknięcia efektu tzw. „treningu negatywnego");
- Wprowadzić i konsekwentnie realizować praktykę organizowania specjalnych treningów (gier zadaniowych) współdziałania koordynatora, organizatorów i wykonawców zadań transportu VIP-ów. Metodykę takich ćwiczeń, na wzór innych gier strategicznych, mogłoby opracować MON, podobnie jak zorganizować w Dęblinie stosowne, wojskowo-cywilne centrum prowadzenia tego typu szkoleń.

- *W sferze technicznej (sprzętowej)*
  - Konieczny jest pilny zakup i wprowadzenie na wyposażenie pułku nowoczesnych samolotów (2 o długim zasięgu i 6 o zasięgu średnim) oraz śmigłowców. Spośród nich co najmniej dwa samoloty i dwa śmigłowce powinny być specjalnie wyposażone jako **powietrzne stanowiska (punkty) kierowania państwem (PSKP)**, z uwzględnieniem wymagań sytuacji krytycznych (kryzysowych i wojennych);
  - W wymaganiach technicznych wobec nowych samolotów dla VIP-ów należy uwzględnić, że wdrożenie zasady rozśrodkowania VIP-ów wskazuje na preferowanie samolotów raczej o stosunkowo mniejszej pojemności;
  - Systematycznie redukować nadzwyczaj niekorzystną dzisiaj różnorodność rodzajów
    i typów sprzętu lotniczego, pozbywając się zwłaszcza pojedynczych egzemplarzy (np. śmigłowiec BELL);
  - Usprawnić i przyspieszyć obsługę serwisową sprzętu pułku. Procedury w tym względzie powinny mieć specjalny chrakter, z uwagi na właśnie specjalny charakter zadań tego pułku związany ze świadczeniem usług dla VIP-ów;
  - Zapewnić budżet pułku stosowny do jego misji i potrzeb zabezpieczenia pełnozakresowego utrzymania sprzętu i szkolenia pilotów.

3. Wykonywanie zadań transportu VIP-ów przez lotnictwo cywilne oraz w warunkach i przypadkach szczególnych

Konieczna jest rozbudowa dotychczasowych zasad i procedur bezpieczeństwa podczas przewozu VIP-ów poprzez uzupełnienie ich co najmniej w dwóch obszarach: a) w razie wykorzystywania do tego celu lotnictwa cywilnego oraz b) w razie wykonywania zadań w przypadkach szczególnych w czasie pokoju, ale przede wszystkim w nadzwyczajnych warunkach kryzysowych i wojennych.

W pierwszym obszarze, tj. w odniesieniu do lotów VIP-ów cywilnymi statkami powietrznymi, należy przede wszystkim w pełni stosować się do obowiązujących powszechnie procedur cywilnych, które każda linia lotnicza musi bezwzględnie przestrzegać. Jest to ograniczenie, któremu każdy VIP musi bezdyskusyjnie się podporządkować, a każdy organizator podróży VIP-a rygorystycznie uwzględnić w planie przedsięwzięcia. Oczywiście transport VIP-ów musi

nakładać także dodatkowe obowiązki na wykonawcę – w tym wypadku linię lotniczą. Dotyczy to w szczególności przypadków czarterowania samolotów.

W drugim obszarze (bezpieczeństwo w przypadkach i warunkach szczególnych) należy uwzględnić konieczność kierowania się w takich sytuacjach zasadami i procedurami odpowiednimi do tych obowiązujących w warunkach kryzysu i wojny. Procedury cywilne muszą wówczas schodzić na dalszy plan. Dla koordynatora, organizatorów i wykonawców oznacza to zwłaszcza:

- W razie lotu z VIP-em na nie w pełni przygotowane lotnisko lub w przewidywaniu nadzwyczaj trudnych warunków atmosferycznych bezwzględnie konieczne jest przeprowadzenie dodatkowych czynności organizacyjnych i zabezpieczających (rekonesans, dodatkowa ochrona, dodatkowe środki łączności, środki ratownicze itp.);
- W razie sytuacji kryzysowej potrzebne będzie wykorzystywanie w większym zakresie państwowych statków powietrznych spoza 36 splt (lotnictwa wojskowego i lotnictwa służb publicznych). Wymagać to może doraźnego doprecyzowania zasad współdziałania, a także uruchomienia u koordynatora i organizatorów odpowiednich struktur (centrum) zarządzania kryzysowego;
- W razie wykonywania zadań w obliczu zagrożeń militarnych lub celowych zakłóceń elektronicznych należało będzie wzmocnić dodatkowo osłonę i obronę statku powietrznego. W warunkach wojennych najważniejsze osoby w państwie korzystać powinny przede wszystkim z Powietrznego Punktu Kierowania, czyli jednego ze specjalnie zawczasu przygotowanych do tego celu statków powietrznych 36 splt.

* * *

Wdrożenie powyższych zaleceń można zapewnić poprzez uwzględnienie ich w całym systemie planowania i programowania, w tym budżetowania, rozwoju sił powietrznych oraz ich bieżącego funkcjonowania, w szczególności w odniesieniu do 36 splt. Dotyczy to także stosownych planów i programów rozwoju i działania BOR.

ZAKOŃCZENIE

Wnioski z analiz systemowych i doświadczenia z reagowania na skutki katastrofy smoleńskiej oraz tegorocznej powodzi wskazują na potrzebę uzupełnienia i skorygowania zasad i procedur zapewniania bezpieczeństwa oraz ciągłości funkcjonowania systemu kierowania państwem w czasie pokoju, kryzysu i wojny. Służyć temu powinno wdrożenie wniosków zawartych w poszczególnych rozdziałach niniejszego raportu[17]. W procesie tym można wyróżnić trzy fazy:

- zmianę niektórych regulacji prawnych i rozwiązań organizacyjnych: od stosownych inicjatyw ustawowych, poprzez modyfikację aktów wykonawczych do nich, aż do korekt w dokumentach organizacyjnych poszczególnych instytucji państwa;
- zapewnienie środków budżetowych i innych zasobów na zrealizowanie zadań wynikających z nowych i zmodyfikowanych koncepcji, planów i programów;
- zorganizowanie szkolenia i zgrywania (treningów) wszystkich podmiotów uczestniczących w realizacji zadań transportu VIP-ów (koordynator, organizatorzy, wykonawcy), zapewniające doskonalenie kadr i struktur oraz weryfikowanie przyjmowanych rozwiązań organizacyjnych i funkcjonalnych.

Niejako dodatkowo, na kanwie wniosków dotyczących poprawy bezpieczeństwa transportu powietrznego ważnych osób w państwie, dadzą się sformułować trzy bardziej ogólne, systemowe propozycje.

[17] Zestawienie potrzebnych działań w tym zakresie przedstawia załącznik nr 8.

Pierwsza wynika z sygnalizowanej w Raporcie potrzeby zbliżenia procedur i wymagań wobec pilotów wojskowych w zakresie transportu VIP-ów do procedur cywilnych. Otóż warto byłoby spojrzeć na ten problem szerzej i podjąć próbę ogolnokrajowej integracji podstawowych obszarów działalności lotnictwa państwowego i cywilnego (niepaństwowego) w jeden spójny system w myśl zasady. Wspólne działania i korzyści z nich mogłyby dotyczyć:

- zintegrowanego, cywilno-wojskowego systemu szkolenia personelu latającego oraz organizacji ruchu lotniczego (wdrożenie procedur ICAO, NATO);
- szeroko pojętej infrastruktury (wyposażanie lotnisk cywilnych i wojskowych w jednorodny sprzęt, jednolity system obsługi urządzeń na lotniskach cywilnych i wojskowych);
- struktur organizacyjnych (tworzenie organów cywilno-wojskowych);
- nowelizacji przepisów prawa (dotychczasowe przepisy stanowią barierę dla procesów integracyjnych – np. brak możliwości przepływu środków finansowych między resortami).

Wydaje się zasadne uruchomienie prac nad takim programem.

Druga propozycja wiąże się z problemem lotnisk zapasowych, które mają istotne znaczenie z punktu widzenia bezpieczeństwa. Dlatego za zasadne należy uznać przygotowanie i utrzymywanie w Warszawie zapasowego lotniska dla VIP-ów, które powinno zapewniać mobilność powietrzną najwyższych władz państwa nawet w razie wyłączenia z użytku lotniska podstawowego. Wydaje się, że rolę taką mogłoby spełniać lotnisko w Modlinie oraz dodatkowo lotnisko Babice-Bemowo. Warto przeprowadzić szerszą analizę tego problemu.

Trzecia propozycja nawiązuje do wciąż niewystarczajacego wykorzystywania wniosków z badania uprzednich wypadków lotniczych. Należałoby więc zastanowić się nad wzmocnieniem kompetencji i zmodyfikowaniem funkcjonowania komisji badania wypadków. Jednym z założeń takiej reformy mogłaby być integracja komisji wypadkowych zmierzająca do ustanowienia jednego, zintegrowanego (ponadresortowego) systemu badania wypadków komunikacyjnych (w tym lotniczych, kolejowych, samochodowych na dużą skalę), czyli powołania rządowej, zintegrowanej komisji wypadkowej.

Wdrażanie wniosków i propozycji zawartych w niniejszym Raporcie przez odpowiednie instytucje państwa powinno nastąpić po uprzednim ich rozpatrzeniu przez Radę Bezpieczeństwa Narodowego. Zadanie monitorowania realizacji wniosków i w razie potrzeby przedkładania raportów dla Rady Bezpieczeństwa Narodowego o stanie ich implementacji należałoby powierzyć Biuru Bezpieczeństwa Narodowego.

Załączniki:

1. *Procedura analizy problemu studyjnego „Bezpieczny VIP";*
2. *Katalog VIP-ów;*
3. *Grupy („koszyki") VIP-ów;*
4. *Obowiązki VIP-a na pokładzie;*
5. *Podstawowe uwarunkowania mobilności powietrznej systemu kierowania państwem;*
6. *Projekt porozumienia w sprawie korzystania z polskich państwowych statków powietrznych przez Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu, Marszałka Senatu oraz Prezesa Rady Ministrów;*
7. *Projekt porozumienia w sprawie zasad bezpieczeństwa lotów statkami powietrznymi lotnictwa cywilnego z najważniejszymi osobami w państwie;*
8. *Sposób implementacji wniosków dotyczących zasad i procedur zapewnienia bezpieczeństwa osób zajmujących ważne (krytyczne) stanowiska państwowe podczas przelotu statkami powietrznymi.*

***

Opracowanie:
Biuro Bezpieczeństwa Narodowego