Stanisław Koziej

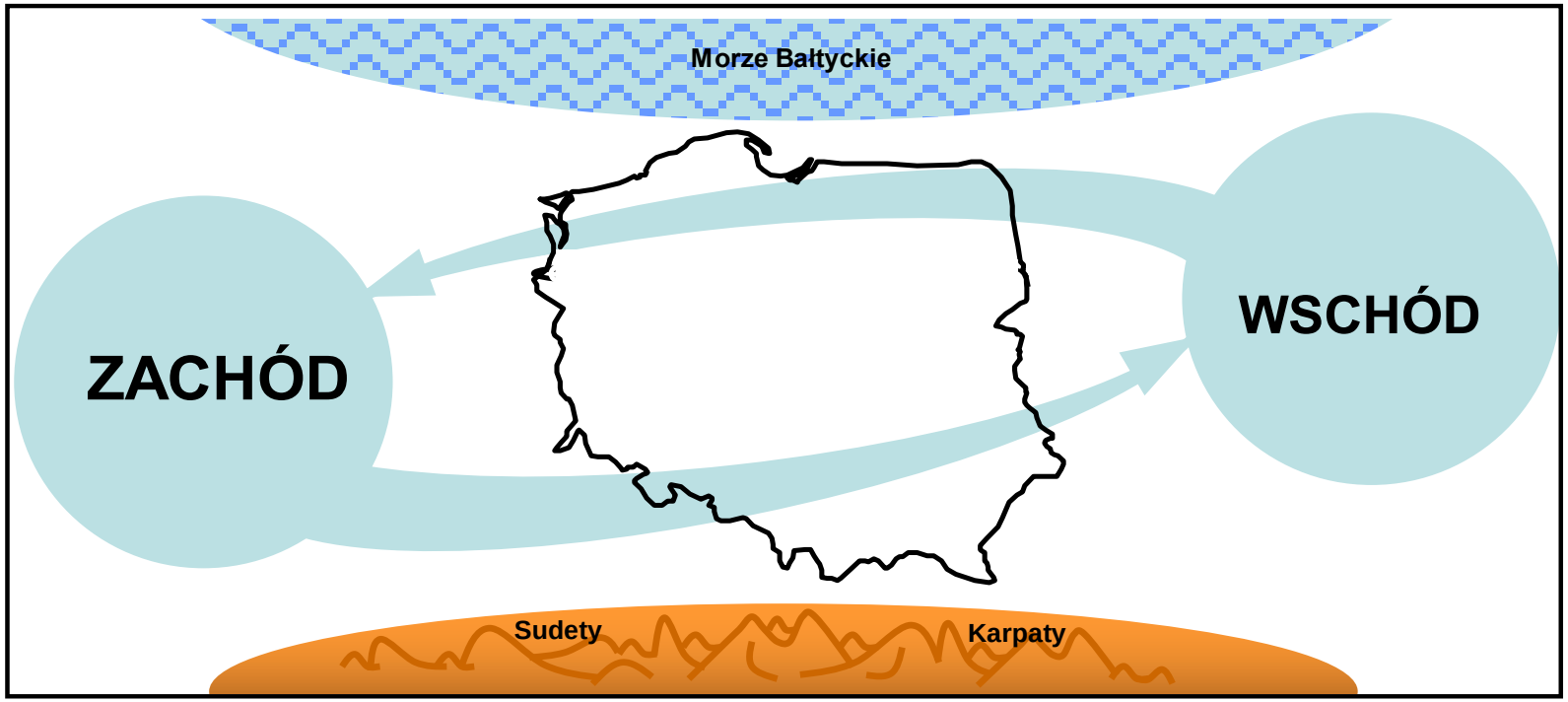
SYSTEM OBRONNY PAŃSTWA

cz. 3 - Działania strategiczne

www.koziej.pl
@SKoziej

Synteza warunków bezpieczeństwa

Geostrategiczne położenie Polski



RODZAJE ZAGROŻEŃ WOJENNYCH
W WARUNKACH HYBRYDOWEJ ZIMNEJ WOJNY – *główna treść konfliktu*

Konfrontacja neozimnowojenna

Rodzaj i skala przemocy | *Progi agresji* | *Rodzaje konfliktu* | *Główna treść konfliktu*

Agresja:

Na pełną skalę

Wojna na pełną skalę

- Bardzo **mało prawdopodobna.** Bezpiecznikiem jest nuklearna zasada MAD (zasada wzajemnego gwarantowanego zniszczenia)
- Nie można jej jednak zupełnie wykluczyć: może być następstwem niekontrolowanej eskalacji („wymknięcia się spod kontroli") wojny ograniczonej, dywersji cybernetycznej „strony trzeciej" w systemach kierowania bronią jądrową, awarii technicznej lub błędu ludzkiego

MAD!!!

Próg wojny nieograniczonej

Ograniczona

Agresja ograniczona
- **wszystkie elementy agresji podprogowej oraz plus:**
- **otwarta agresja zbrojna o deklarowanych celach ograniczonych „parasol" w postaci szantażu użyciem taktycznej broni jądrowej (doktryna „deeskalacji nuklearnej")**

Deeskalacja nuklearna TBJ

Próg otwartej agresji (ograniczonej)

Skryta

Agresja poniżej progu wojny
- **wszystkie elementy presji oraz plus:**
- **operacje specjalne, dywersja, prowokacje zbrojne...**

Sytuacja trudnokonsensusowa

Próg skrytej agresji

Presja

Presja polityczno-militarna

- Agresywna dyplomacja (coercive diplomacy)
- Wojna informacyjna – dezinformacja, propaganda, media, media społecznościowe ...
- Cyberkonfrontacje – cyberdywersja, groźba cyberwojny
- Szantaż ekonomiczny (np. energetyczny, sankcje)
- Manewry wojskowe
- Prowokacyjne incydenty wojskowe
- Wojny zastępcze (proxy wars)

Próg presji

Wojna:

Na pełną skalę

ZAGŁADA TOTALNA

ODSTRASZANIE NUKLEARNE

Ograniczona

Kontrola eskalacji

ODSTRASZANIE KONWENCJONALNE

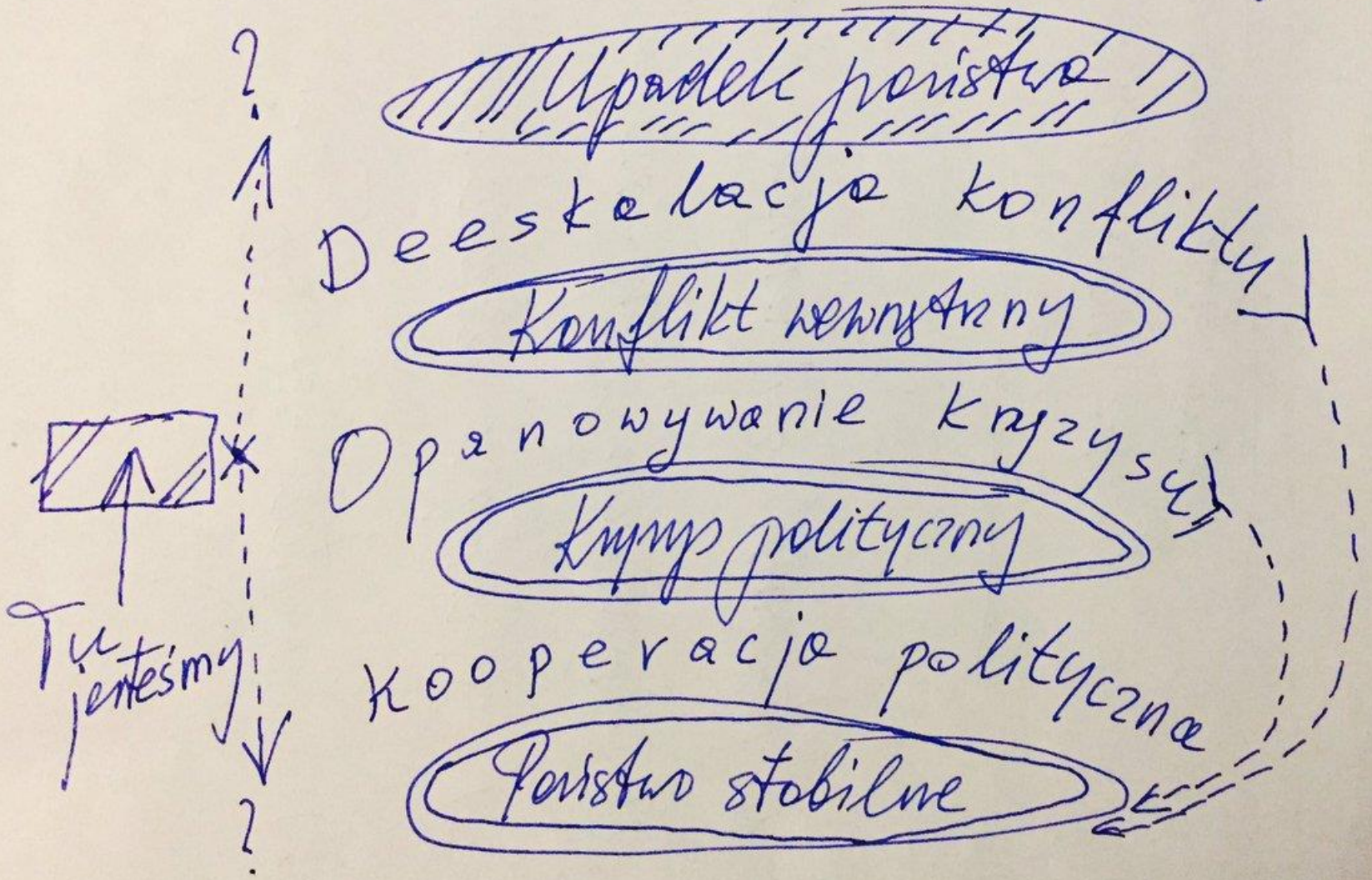
Skryta

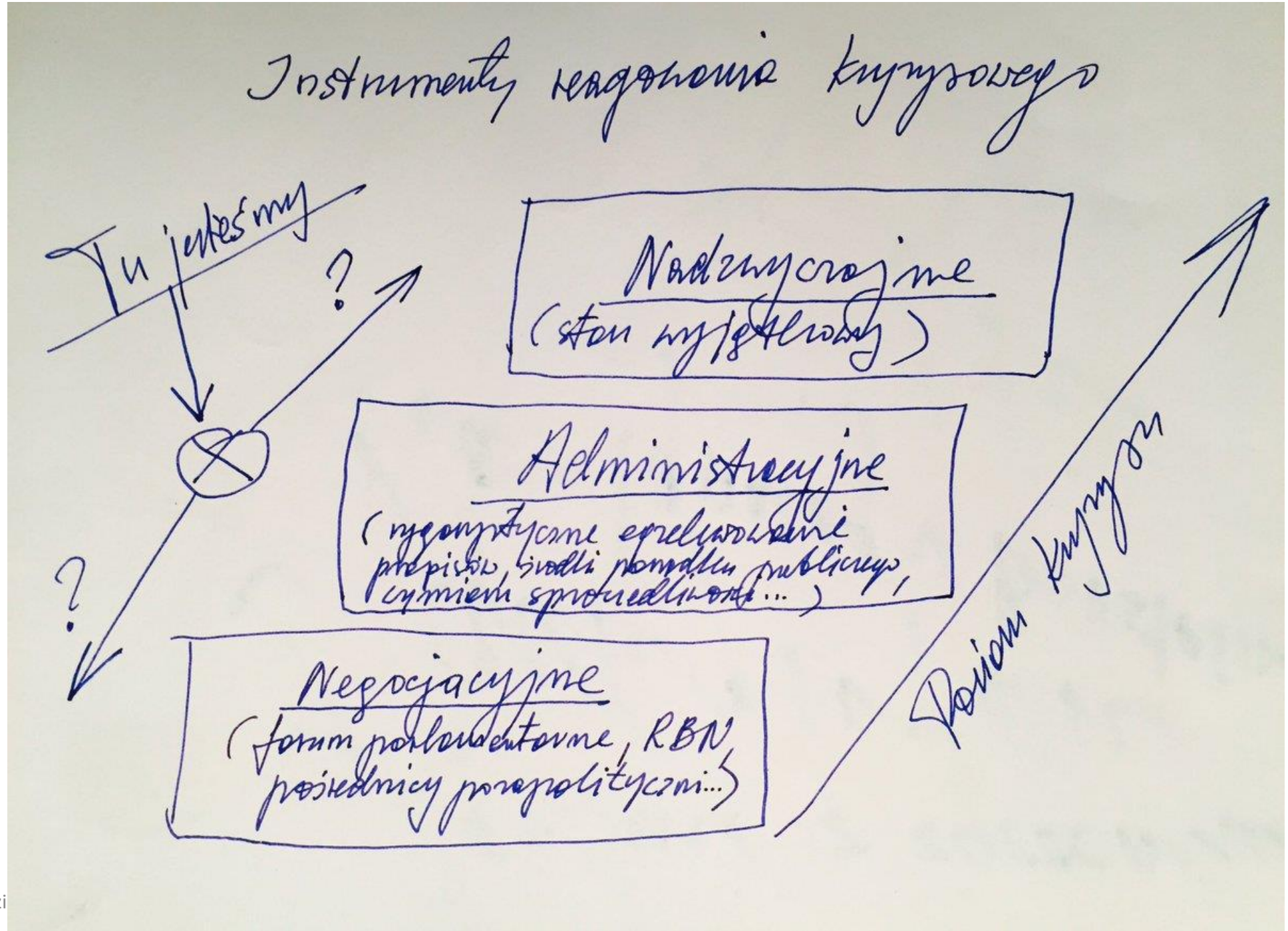
Kryzys

Reagowanie kryzysowe

Kooperacja pozimnowojenna

Matryca bezpieczeństwa wewnętrznego państwa




Instrumenty reagowania kryzysowego
Tu jesteśmy
?
?
Nadzwyczajne
(stan wyjątkowy)
Administracyjne
(nieoptymalne egzekwowanie przepisów, siodła nomadów publicznych, czynienie sprawiedliwości...)
Negocjacyjne
(forum parlamentarne, RBN, pośrednicy parapolitycznie...)
Poziom kryzysu

Koncepcja strategii operacyjnej

Strategia operacyjna - opcje

1. **Maksymalnego umiędzynarodowienia działań na rzecz bezpieczeństwa Polski, związana także z przesunięciem uwagi na działania pozamilitarne;**

2. **Autarkii strategicznej (samodzielności i samowystarczalności): zakłada zdecydowane wzmocnienie samodzielności działania państwa w sferze bezpieczeństwa w kontekście kryzysu zbiorowej polityki bezpieczeństwa w Europie i we wspólnocie transatlantyckiej, z dominacją uwagi na „twardym" bezpieczeństwie;**

3. **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 nie może być gwarantowana.**

Strategia operacyjna - priorytety

1. **Utrzymanie własnej determinacji i gotowości do działania (podmiotowość strategiczna!)** w pełnym spektrum dziedzin, obszarów i sektorów bezpieczeństwa narodowego z priorytetowym traktowaniem tych, w których sojusznicze (wspólne) działanie może być utrudnione (sytuacje trudnokonsensusowe);

2. **Umacnianie międzynarodowej wspólnoty bezpieczeństwa** poprzez działanie na rzecz pogłębiania procesów integracyjnych w Europie opartych na **wspólnocie interesów** (konsolidacja NATO, wspólnota interesów w UE, partnerstwa strategiczne, w tym z USA);

3. **Wspieranie i selektywny udział w międzynarodowym reagowaniu kryzysowym** (prewencja, stabilizacja), przeciwdziałającej powstaniu nowych źródeł zagrożeń lub rozprzestrzenianiu się już istniejących kryzysów w wymiarze ponadregionalnym.

Rodzaje działań (operacji) strategicznych

- **pogotowie strategiczne (działania zapobiegawcze)** - realizowane w czasie pokoju, obejmujące promowanie bezpieczeństwa, bieżące zapobieganie wystąpieniu zagrożeń poprzez neutralizowanie ich potencjalnych źródeł oraz umacnianie bezpiecznego środowiska (otoczenia) międzynarodowego Polski
- **reagowanie kryzysowe** - realizowane w razie wystąpienia zagrożenia bezpieczeństwa państwa lub bezpieczeństwa sojuszników oraz zagrożeń dla szerszego bezpieczeństwa międzynarodowego, obejmujące zarówno działania narodowe, jak i udział w wysiłkach międzynarodowych, podejmowanych w celu opanowania kryzysów oraz zapewnienia osłony przed ich skutkami
- **działania wojenne** - prowadzone w razie agresji na Polskę lub jej sojuszników, obejmujące wykorzystanie całego lub części potencjału państwa do odparcia agresji, poprzez przygotowanie i przeprowadzenie kampanii i operacji wojennych

DZIAŁANIA WOJENNE

(Następstwo agresji na Polskę lub sojusznika. W sensie prawnym każda „polska” wojna byłaby wojną sojuszniczą)

Wojna obronna na własnym terytorium (odparcie agresji na Polskę):

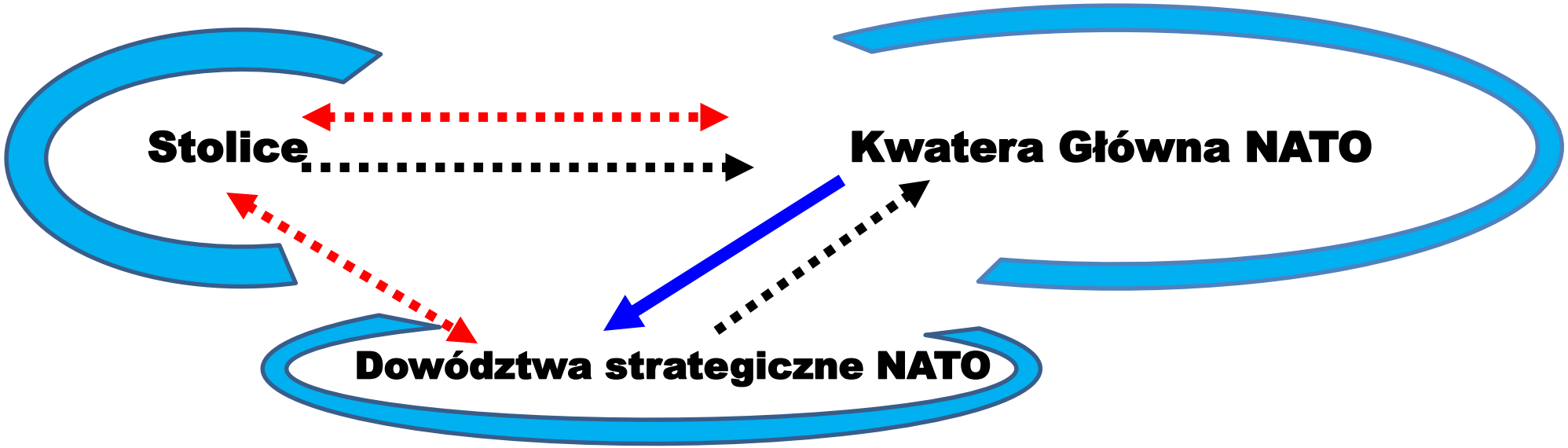
- **agresja skryta (podprogowa)**
- **agresja ograniczona (np. aterytorialna)**
- **wojna na dużą skalę**

Wojna poza terytorium RP (udział w odparciu agresji na sojusznika)

- **Działania zbrojne**
- **Działania pozazbrojne**

Działania w ramach sojuszu

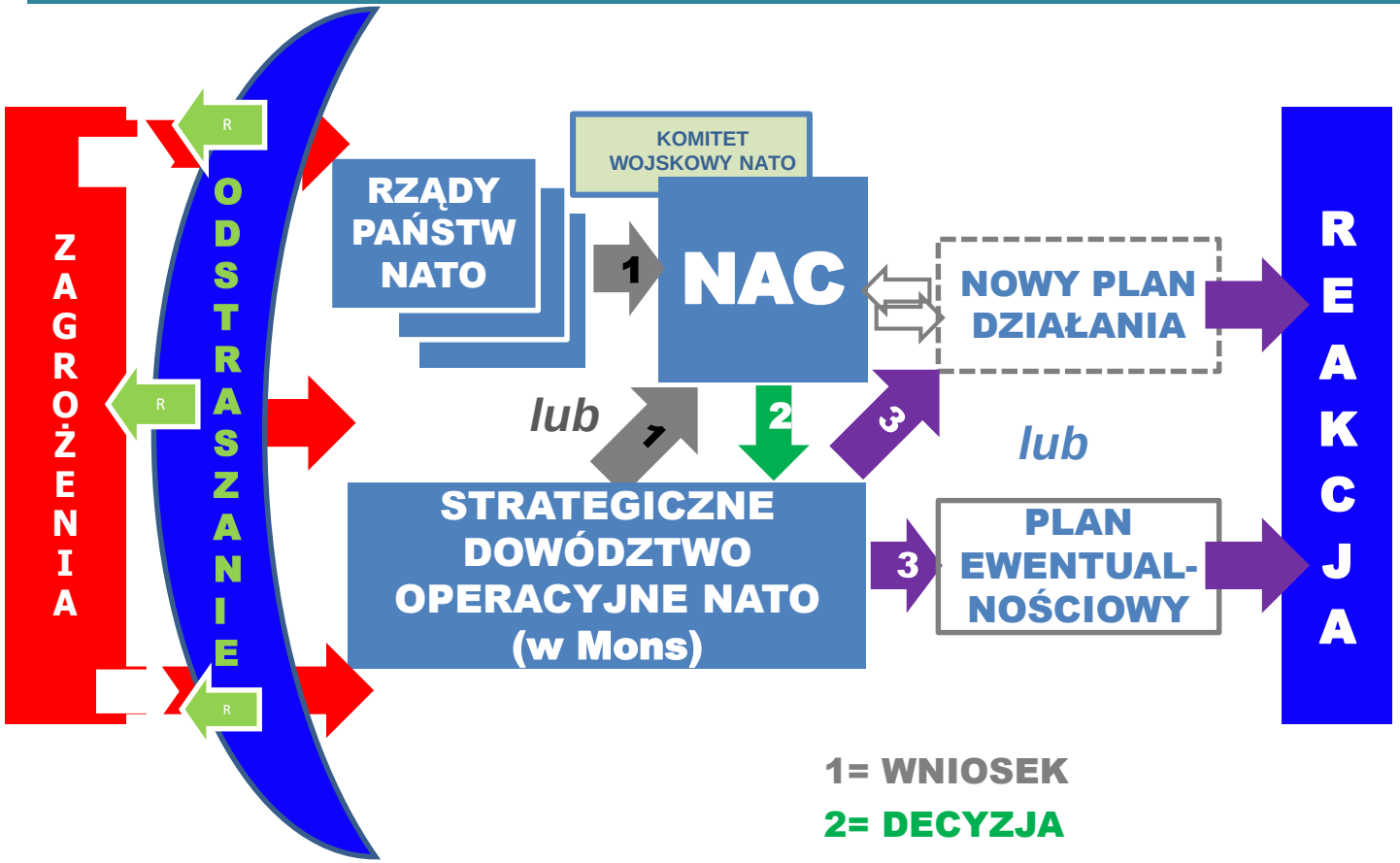
PROCEDURY



- ------ **wnioski, propozycje**
- ------ **konsultacje**
- ------ **decyzje**

  - **Ciągłe konsultacje w sprawach bieżących (stolice – Kwatera Główna – dowództwa strategiczne)**

Mechanizm reagowania NATO



1= WNIOSEK

2= DECYZJA

3= DZIAŁANIE

(*plan i realizacja*)

Potrzeba adekwatnej strategii i potencjału odstraszania

- **Jak w klasycznej zimnej wojnie XX wieku warunkiem utrzymania konfrontacji na poziomie poniżej gorącej wojny jest równowaga odstraszania**
- **Dzisiaj takiej równowagi brak. Rosja ma przewagę w hybrydowej zimnej wojnie i istnieje spore ryzyko przekształcenia się jej w gorącą**
- **Stąd wynika konieczność zbudowania przez Zachód (NATO+UE) adekwatnej strategii i potencjału odstraszania**

Kwadryga odstraszania

SIŁY NUKLEARNE: strategiczne – doktryna MAD, taktyczna broń jądrowa w Europie – wzmocniony program „nuclear sharing”)

SIŁY KONWENCJONALNE: wysunięta obecność („czata”), siły reagowania (w tym „szpica” – z doktryną uprzedzającego rozwinięcia), siły wzmocnienia (plany ewentualnościowe i weryfikujące je manewry)

Odstraszanie w warunkach hybrydowej zimnej wojny

POTENCJAŁ INFORMACYJNY: konieczność zbudowania strategii i potencjału walki informacyjnej (system komunikacji strategicznej, cyberobrona: współpraca NATO-UE)

@SKoziej

ODPORNOŚĆ STRATEGICZNA : obrona powietrzna, w tym p/rakietowa (zdolności A2/AD); operacyjne przygotowanie terytorium; ochrona i obrona ważnych obiektów infrastruktury krytycznej; potencjał mobilizacyjny; przygotowanie państwa podziemnego, w tym zbrojnego oporu/dywersji, na terytoriach okupowanych; system ochrony ludności w warunkach wojny; powszechna edukacja w sprawach bezpieczeństwa

Nuclear Sharing

Program NATO wspólnego używania broni jądrowej przez USA i europejskich sojuszników niemających własnych arsenałów odstraszania nuklearnego

Państwo gospodarz rozmieszczenia bomb jądrowych USA	Baza sił powietrznych	Liczba bomb jądrowych USA	Samoloty państwa gospodarza zdolne przenosić bomby jądrowe USA	
			obecnie	planowana nowa generacja
BELGIA	Kleine Brogel	10–20	F-16 **koniec żywotności w latach 2023–2031**	**decyzja niepodjęta**
HOLANDIA	Volkel	10–20	F-16	F-35
WŁOCHY	Aviano	w przybliżeniu 50	Tornado	F-35
	Ghedi	20–40		
NIEMCY	Büchel	20 lub więcej	Tornado **do 2020 roku**	**po 2020 roku brak – Tornada będą zastąpione Tajfunami bez zdolności przenoszenia bomb jądrowych USA**
TURCJA	Incirlik	50–90	F-16	F-35
RAZEM	**5 państw 6 baz**	**160–240 bomb – najbardziej prawdopodobnie 180**		

CYBERBEZPIECZEŃSTWO W RAMACH NATO

- **Cyberobrona jest częścią obrony kolektywnej na podstawie art.5. tak, jak obrona lądzie morzu i w powietrzu (szczyt w Warszawie)**
- **NATO uznaje, że prawo międzynarodowe stosuje się również odpowiednio do cyberprzestrzeni (Podręcznik „talliński” z 2013r.).**
- **NATO odpowiada za ochronę własnych sieci informatycznych oraz koordynację wysiłków narodowych, a także rozwój edukacji i ćwiczeń w zakresie cyberobrony.**
- **Państwa sojusznicze zobowiązały się do ochrony swoich sieci, wymiany informacji oraz wzajemnego wsparcia w zakresie cyberobrony (zapobieganie, powstrzymywanie, likwidacja skutków cyberataków), a także rozwijania swoich zdolności kompatybilnych w NATO (Warszawa).**
- **NATO podpisało porozumienie o cyber-współpracy z UE (TANDEM)**

UNIA EUROPEJSKA
IMPLEMENTATION PLAN ON SECURITY AND DEFENCE: Level of ambitions

- **Responding to external conflicts and crises** ***(cywilne i wojskowe reagowanie kryzysowe)***
- **Building the capacities of partners** ***(misje szkoleniowo-doradcze w sektorze bezpieczeństwa)***
- **Protecting the Union and its citizens** ***(ochrona i odporność państw i obywateli na różnorodne zagrożenia)***

EUROPEAN DEFENCE ACTION PLAN
(Propozycja Komisji Europejskiej, 30.11.2016)

- **Launching a European Defence Fund**
  - **„Research window” (unijne, wspólne projekty badawcze)**
  - **„Capability window” (współpraca przemysłowa: dwa poziomy – dla wszystkich i dla chętnych)**
- **Fostering investments in defence supply chains (inwestycje, innowacje…)**
- **Reinforcing the single market for defence (otwartość, konkurencyjność rynku …)**

Wspólny zestaw zadań współpracy NATO-UE

1. **Countering hybrid threats**
2. **Operational cooperation including maritime issues**
3. **Cyber security and defence**
4. **Defence capabilities**
5. **Defence industry and research**
6. **Exercises**
7. **Defence and security capacity-building**

UNIA EUROPEJSKA: perspektywa

- **W sumie:**
  - **NATO- bis? – NIE; *chyba że NATO miałoby się rozpadać!!!***
  - **UE dwóch kręgów (prędkości, poziomów)? – RYZYKO DLA POLSKI; *dlatego potrzeba przyjęcia strategii/doktryny CSDP***
  - **Tandem NATO/UE? – TAK; *rozwiązanie optymalne!***

Misja strategiczna UE – jako synteza interesów narodowych państw członkowskich

Interesy państw członkowskich i stosunek do nich innych państw (partnerów, sojuszników):

- **Wspólne (akceptowane) – wszyscy są gotowi uczestniczyć w we wsparciu ich realizacji (ubezpieczane wspólnotowo);**
- **Niesprzeczne (tolerowane) – nikt nie zgłasza wobec nich sprzeciwu, ale też nie deklaruje z góry udziału w zabezpieczeniu ich realizacji (w razie potrzeby – koalicja ad hoc);**

Katalog (pakiet) wspólnych i niesprzecznych interesów państw członkowskich, czyli:

Misja UE w dziedzinie bezpieczeństwa

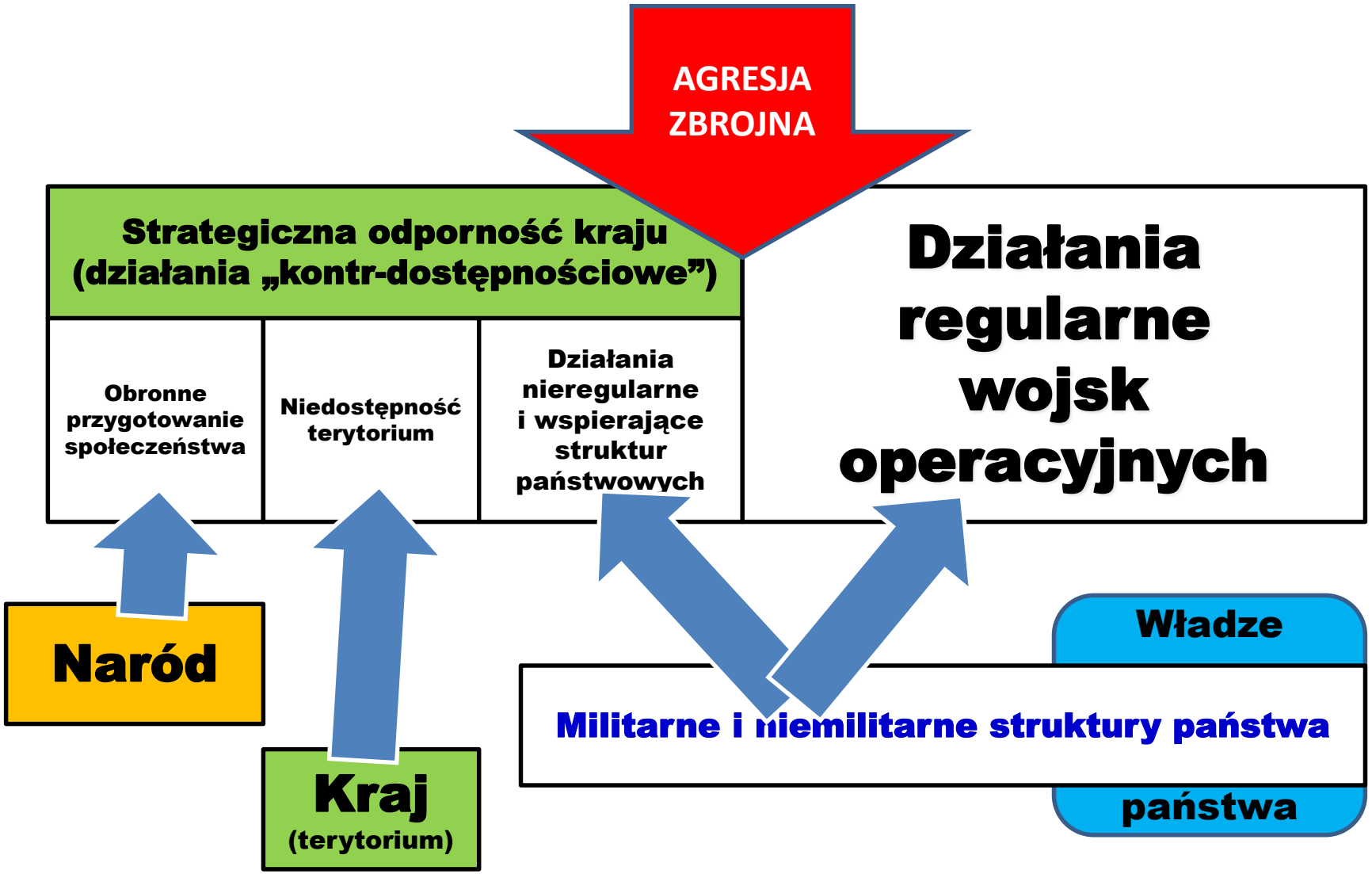
- **Sprzeczne (odrzucone) – nie uwzględniane we wspólnej misji bezpieczeństwa.**

Działania narodowe

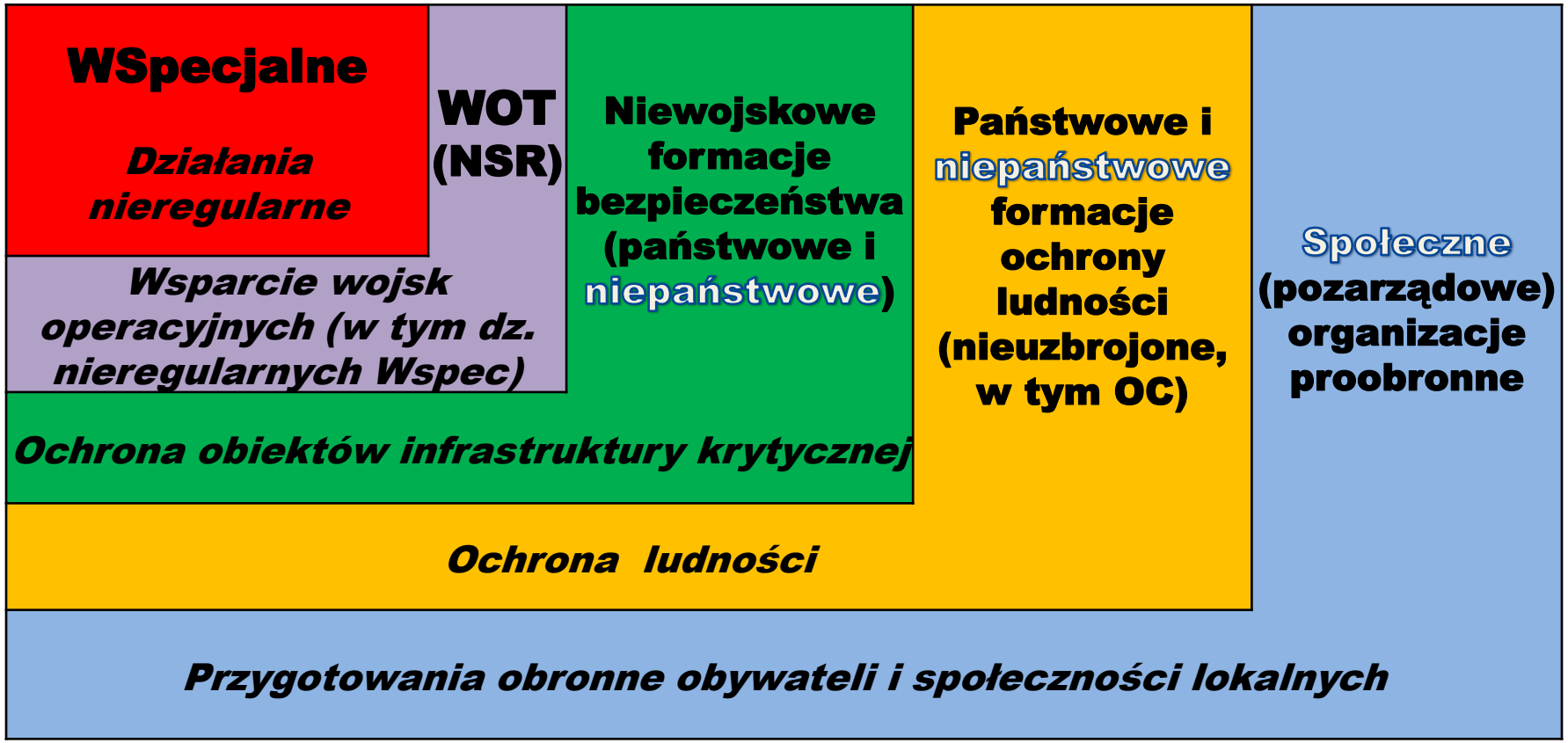
DZIAŁANIA STRATEGICZNE (STRATEGIA OPERACYJNA)

- **Pogotowie (ubezpieczenie) strategiczne**
  - **Współpraca sojusznicza i partnerstwa**
  - **Wywiad i kontrwywiad**
  - **Przygotowania obronne**
- **Reagowanie kryzysowe**
  - **Pozamilitarne (dyplomacja, sankcje …)**
  - **Polityczno-militarne (udział w misjach, manewry…)**
- **Obrona (działania wojenne)**
  - **Agresja na dużą skalę – obrona sojusznicza**
  - **Agresja ograniczona - udział w obronie sojusznika**
  - **Agresja skryta (podprogowa) – obrona samodzielna i/lub sojusznicza**

O B R O N A P A Ń S T W A

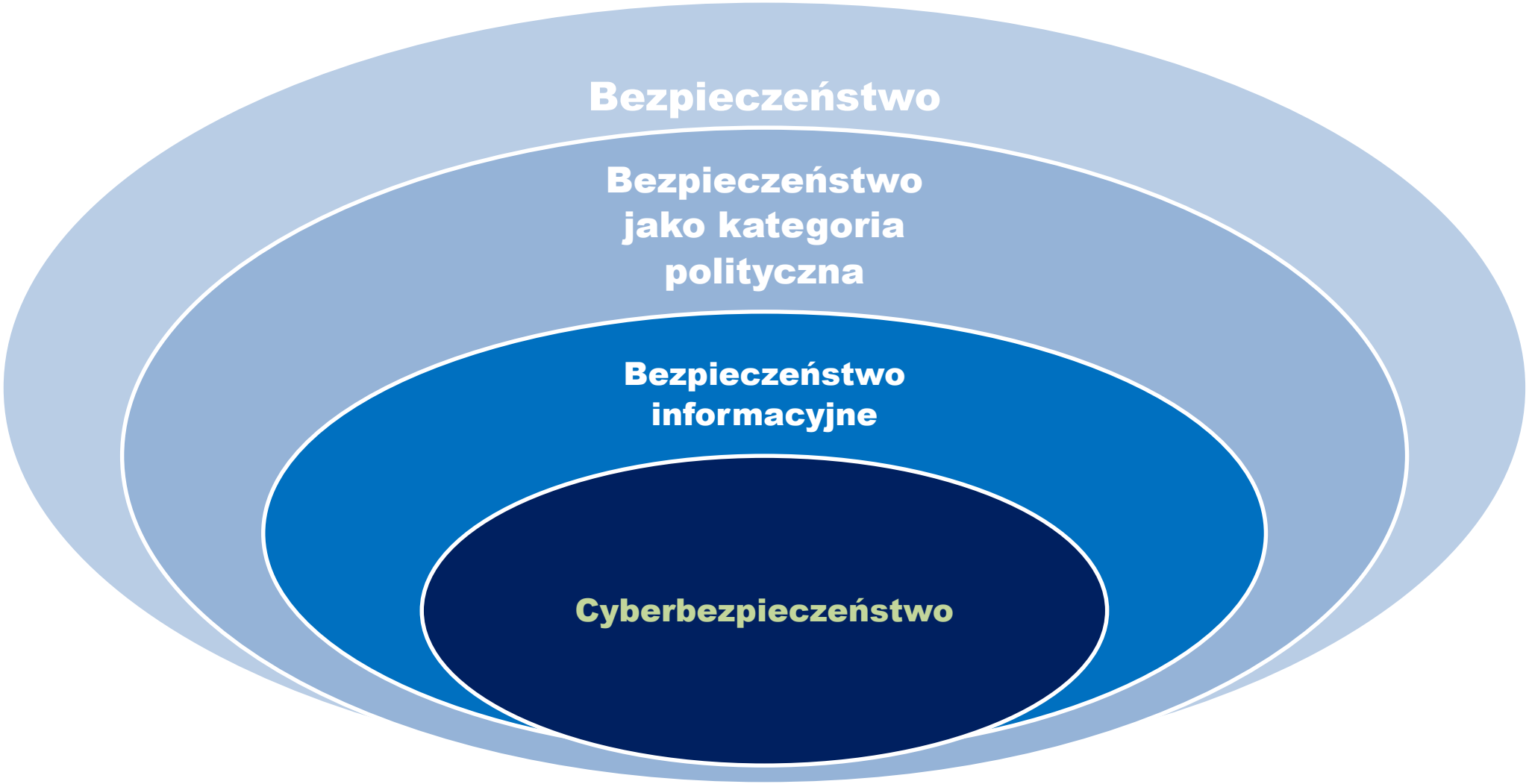


Siły i środki
SYSTEMU STRATEGICZNEJ ODPORNOŚCI KRAJU



Cyberbezpieczeństwo

Cyberbezpieczeństwo jako rodzaj bezpieczeństwa



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 realizację 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.

Cyberbezpieczeństwo państwa (bezpieczeństwo państwa w cyberprzestrzeni) - transsektorowy obszar bezpieczeństwa, obejmujący proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego elementów (struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej) oraz będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych.

Rozróżnienie pojęć:

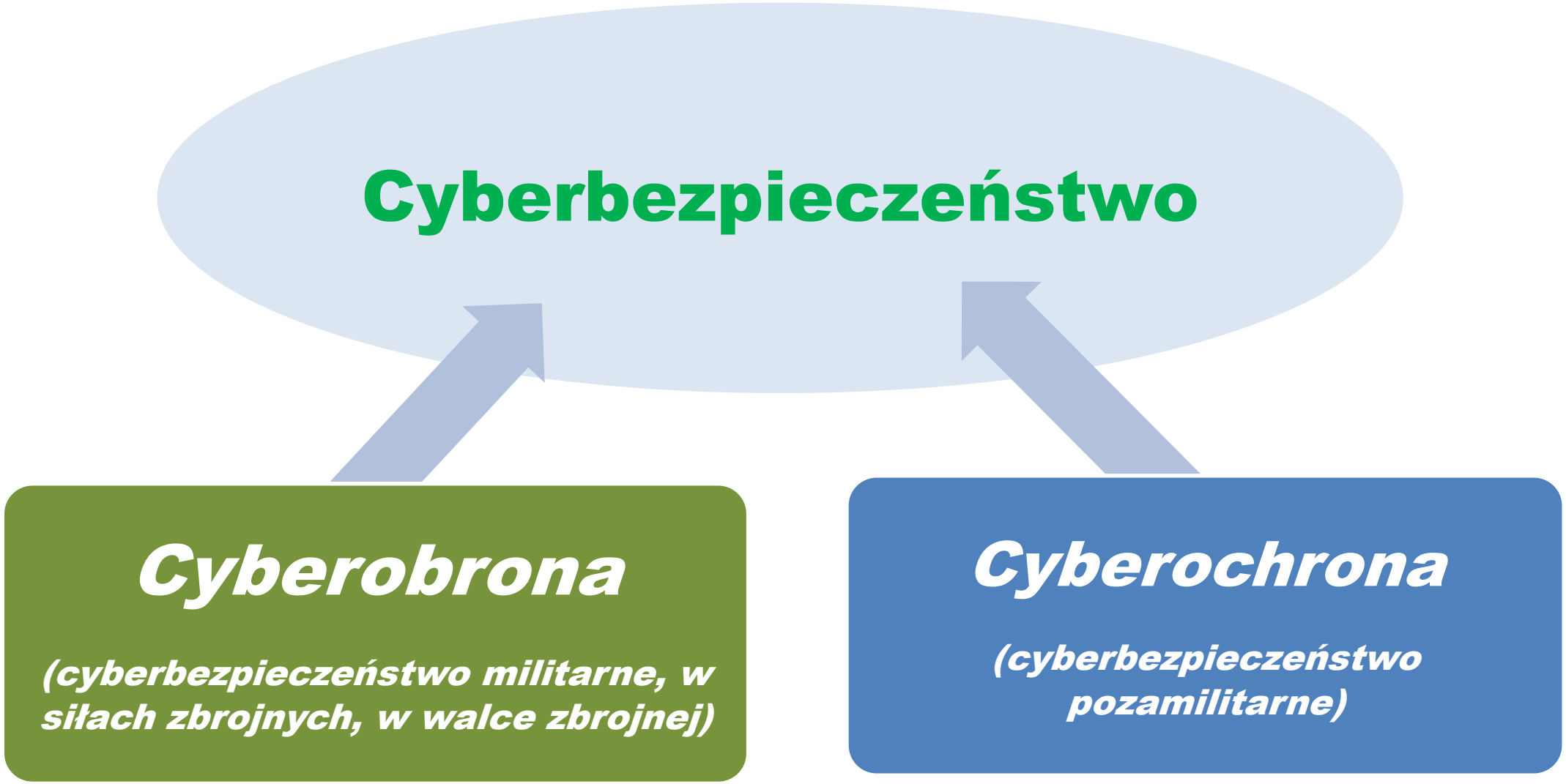
„BEZPIECZEŃSTWO PAŃSTWA W CYBERPRZESTRZENI”

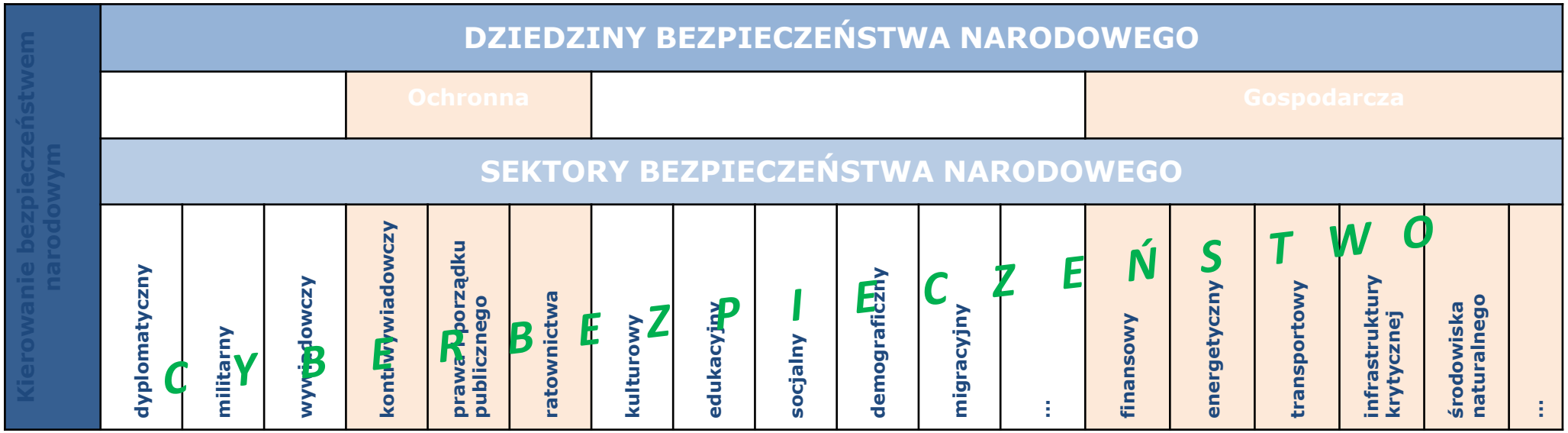
oraz

„BEZPIECZEŃSTWO CYBERPRZESTRZENI PAŃSTWA”

(raczej ochrona cyberprzestrzeni)

CYBERBEZPIECZEŃSTWO A CYBEROBRONA I CYBEROCHRONA





- Struktury rządowe
- Struktury samorządowe
- Podmioty prywatne (pozapaństwowe, pozarządowe)
- Obywatele

Cyberbezpieczeństwo w procesie planowania strategicznego (w cyklu strategicznym)

Doktryna cyberbezpieczeństwa RP

- **Strategiczny cel operacyjny:** zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni
  - Ustawa o cyber- w stanach nadzwyczajnych
  - PSDO, plany operacyjne, ćwiczenia
- **Strategiczny cel preparacyjny:** zbudowanie zintegrowanego systemu cyberbezpieczeństwa RP
  - Rządowa Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020
  - Rozwój zdolności cyberobrony w siłach zbrojnych

POSUMOWANIE
STRATEGII BEZPIECZEŃSTWA NARODOWEGO RP

- **Skoncentrowanie głównego wysiłku na zapewnieniu bezpośredniego bezpieczeństwa, w tym obrony państwa i wzmocnieniu strategicznej odporności kraju (na agresję)**
- **Własny potencjał obronny – podstawowy filar i gwarancja polskiego bezpieczeństwa; NATO, UE, strategiczne partnerstwa – filary wspierające**
- **Zdolności do obrony terytorium i przeciw-zaskoczeniowe – polska specjalizacja w NATO i UE**
- **Potrzeba umacniania podmiotowości strategicznej na arenie międzynarodowej**