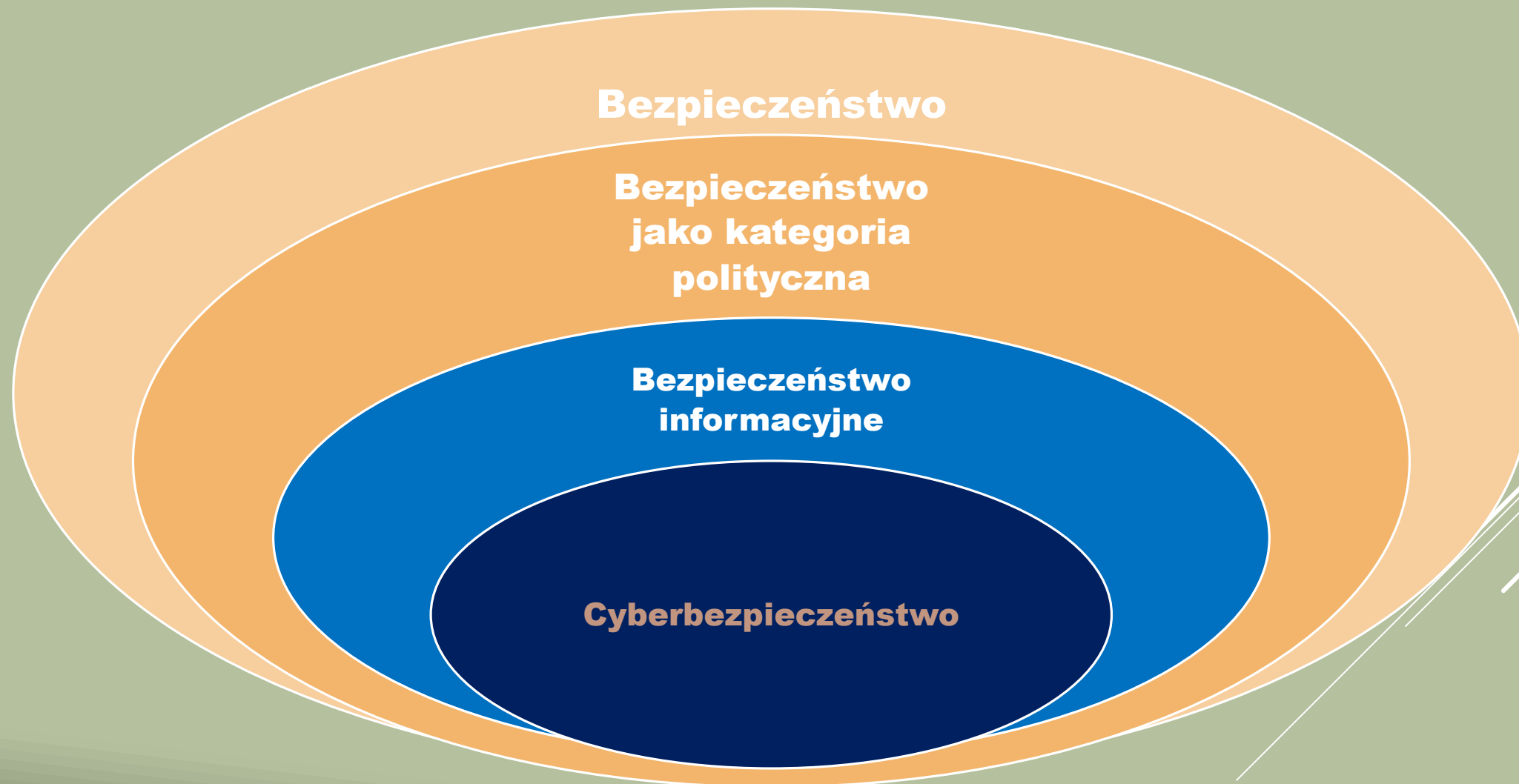


*Stanisław Koziej*

# **WIELOWYMIAROWOŚĆ (KOMPLEKSOWOŚĆ) CYBERBEZPIECZEŃSTWA**

# 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

**Cyberbezpieczeństwo**



***Cyberobrona***

*(cyberbezpieczeństwo militarne, w siłach zbrojnych, w walce zbrojnej)*

***Cyberochrona***

*(cyberbezpieczeństwo pozamilitarne)*

# TRANSSEKTOROWOŚĆ I WIELOPOZIOMOWOŚĆ CYBERBEZPIECZEŃSTWA

Kierowanie bezpieczeństwem narodowym	DZIEDZINY BEZPIECZEŃSTWA NARODOWEGO																
	Obronna		Ochronna		Społeczna				Gospodarcza								
	SEKTORY BEZPIECZEŃSTWA NARODOWEGO																
	dyplomatyczny	militarny	wywiadowczy	kontrowiadowy	prawa i porządku publicznego	ratownictwa	kulturowy	edukacyjny	socjalny	demograficzny	migracyjny	...	finansowy	energetyczny	transportowy	infrastruktury krytycznej	środowiska naturalnego

**CYBERBEZPIECZEŃSTWO**

**Struktury rządowe**

**Struktury samorządowe**

**Podmioty prywatne**

**Obywatele**

# WIELOETAPOWOŚĆ (WIELOFAZOWOŚĆ) CYBERBEZPIECZEŃSTWA

REALIZACJA



PRZYGOTOWANIE



# Cyberbezpieczeństwo w procesie planowania strategicznego (w cyklu strategicznym)



# GLOBALNOŚĆ CYBERBEZPIECZEŃSTWA

**TRANSNARODOWOŚĆ**

**TRANSGRANICZNOŚĆ**

**TRANSSPOŁĘCZNOŚĆ**

**TRANSKULTUROWOŚĆ**

**TRANSCYWILIZACYJNOŚĆ**

.....

# DOKTRYNA CYBERBEZPIECZEŃSTWA RP

- **Strategiczny cel operacyjny:** zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni
  - Ustawa o cyber- w stanach nadzwyczajnych
  - PSDO, plany operacyjne, ćwiczenia – **potrzeba uwzględniania!**
- **Strategiczny cel preparacyjny:** zbudowanie zintegrowanego systemu cyberbezpieczeństwa RP
  - Krajowe Ramy Polityki Cyberbezpieczeństwa RP
  - Rozwój zdolności cyberobrony w siłach zbrojnych (w tym kryptologia!)

# PRZYKŁAD PROBLEMU: SUWERENNOŚĆ W CYBERPRZESTRZENI

- **Wysoce z informatyzowane systemy walki i wsparcia (WZSWiW), np.:**
  - **systemy przeciw rakietowe, przeciwlotnicze, broń inteligentna (precyzyjna), bezzałogowce, samoloty, śmigłowce, okręty podwodne (rakiety i torpedy) ...**
- **Pewność wykorzystania takiego sprzętu zależy od pełnego dysponowania ich podsystemami informatycznymi („panowanie cyber/informatyczne”)**
- **Dlatego przy zakupach obcych wysoce z informatyzowanych systemów broni „priorytetem priorytetów” musi być uzyskanie dostępu do tzw. „kodów źródłowych”**

# 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)**

# CYBERBEZPIECZEŃSTWO W HYBRYDOWEJ ZIMNEJ WOJNIE

- **Cyberbezpieczeństwo – coraz istotniejsza część zmaganiań informacyjnych w warunkach nowej, **hybrydowej zimnej wojny** (cyberinterwencje polityczne, np. w wybory, szpiegostwo gospodarcze, cyberprzestępczość ...)**
- **Potencjał cyberbezpieczeństwa NATO – składnik strategicznej **triady odstraszania**:**
  - **Potencjał informacyjny (komunikacji strategicznej), w tym **cyberbezpieczeństwa** (pilna potrzeba budowy!)**
  - **Siły konwencjonalne**
  - **Siły nuklearne: **problem wpływu cyber-środowiska na odstraszanie nuklearne****

# DZIĘKUJĘ