

Wstęp

Rozdział I. *Koncepcja zagrożeń asymetrycznych i jej miejsce w teorii stosunków międzynarodowych oraz nauce o bezpieczeństwie*

1. Ewolucja pojęcia 'bezpieczeństwo' w teorii stosunków międzynarodowych oraz w nauce o bezpieczeństwie (security studies)
 - 1.1. Ogólne rozumienie pojęcia 'bezpieczeństwo' w nauce o stosunkach międzynarodowych
 - 1.2. Tradycyjne (realistyczne) rozumienie pojęcia 'bezpieczeństwo' – paradygmat zimnowojenny
 - 1.3. Współczesne rozumienie pojęcia 'bezpieczeństwo' – elementy formułującego się paradygmatu pozimnowojennego
2. Źródła koncepcji zagrożeń asymetrycznych w wojskowej myśli strategicznej
 - 2.1. Ogólne rozumienie asymetrii w nauce o strategii
 - 2.2. Korzenie koncepcji asymetrii w historii myśli strategicznej
 - 2.3. Obecne pojmowanie asymetrii w wojskowej myśli strategicznej
3. Definiowanie zagrożeń asymetrycznych
 - 3.1. Zagrożenia asymetryczne sensu largo (ujęcie wojskowe)
 - 3.2. Zagrożenia asymetryczne sensu stricto (ujęcie politologiczne)
4. Ogólna charakterystyka zagrożeń asymetrycznych (węższe ujęcie)
5. Zachodocentryzm koncepcji zagrożeń asymetrycznych

Rozdział II. *Uwarunkowania rozwoju i czynniki kształtujące środowisko działania podmiotów stanowiących zagrożenia asymetryczne*

1. Globalny kontekst działania podmiotów stanowiących zagrożenia asymetryczne – przemiany ładu międzynarodowego i nowe osie podziałów
 - 1.1. Koniec zimnej wojny i rozpad dwubiegunowego ładu międzynarodowego
 - 1.2. Wertykalizacja porządku międzynarodowego na płaszczyźnie socjoekonomicznej
 - 1.3. Zróżnicowanie kulturowo-cywilizacyjne społeczności międzynarodowej
2. Główne czynniki bezpośrednio wpływające na środowisko działania podmiotów stanowiących zagrożenia asymetryczne – procesy globalizacyjne i postęp technologiczny
 - 2.1. Globalizacja (procesy globalizacyjne) – podstawowe elementy pojęcia
 - 2.2. Erozja suwerenności państwowej i problem państw w stanie rozkładu
 - 2.3. Swoboda przepływów transgranicznych towarów, kapitału i ludzi oraz kwestia migracji międzynarodowych
 - 2.4. Wzrost wrażliwości państw na działania podmiotów stanowiących zagrożenia asymetryczne. Rola mediów
 - 2.5. Procesy globalizacyjne i ich następstwa jako motyw rozwoju zagrożeń asymetrycznych
3. Przemiany w sferze wojskowej stosunków międzynarodowych a środowisko działania podmiotów stanowiących zagrożenia asymetryczne
 - 3.1. Specyfika współczesnych konfliktów zbrojnych
 - 3.2. Dysproporcje potencjałów wojskowych na świecie, znaczenie postępu technologicznego oraz kwestia rewolucji w dziedzinie wojskowości (RMA)

Rozdział III. *Terroryzm międzynarodowy jako zagrożenie asymetryczne państw obszaru transatlantyckiego*

1. Terroryzm – kwestie definicyjne
2. Aspekt motywacyjny terroryzmu – specyfika w okresie pozimnowojennym

- 2.1. Religijna motywacja działań terrorystycznych – ogólna charakterystyka i obecne znaczenie
- 2.2. Terroryzm ugrupowań islamskich – znaczenie w wymiarze motywacyjnym
- 2.3. Inne motywacje działań terrorystycznych w okresie pozimnowojennym
3. Organizacja i finansowanie działań terrorystycznych – główne trendy rozwojowe
 - 3.1. Struktura współczesnych grup terrorystycznych
 - 3.2. Finansowanie działalności terrorystycznej
 - 3.3. Wsparcie ze strony państw (sponsoring państwowy)
4. Płaszczyzna operacyjna – zmiany w zakresie środków i taktyk ataku
5. Ocena strategicznej rangi zagrożenia ze strony terroryzmu międzynarodowego dla państw obszaru transatlantyckiego

Rozdział IV. *Transnarodowa przestępczość zorganizowana jako zagrożenie asymetryczne*

1. Istota i specyfika transnarodowej przestępczości zorganizowanej
 - 1.1. Definiowanie transnarodowej przestępczości zorganizowanej
 - 1.2. Specyfika wpływu transnarodowej przestępczości zorganizowanej na bezpieczeństwo państw
2. Płaszczyzna organizacyjna – cechy specyficzne transnarodowej przestępczości zorganizowanej
 - 2.1. Usieciowienie i decentralizacja – główny trend rozwojowy w aspekcie techniczno-organizacyjnym
 - 2.2. Pozostałe tendencje rozwojowe w wymiarze organizacyjnym. Sojusze strategiczne i współpraca grup przestępczych z innymi podmiotami pozapaństwowymi
3. Główne obszary aktywności kryminalnej transnarodowych grup przestępczych
 - 3.1. Handel narkotykami
 - 3.2. Inne formy aktywności przestępczej
4. Próba oceny rangi zagrożenia ze strony transnarodowej przestępczości zorganizowanej dla bezpieczeństwa państw transatlantyckich

Rozdział V. *Użycie przez podmioty pozapaństwowe środków niekonwencjonalnych (broni masowego rażenia – BMR)*

1. Pojęcie i rodzaje broni masowego rażenia – BMR (Weapons of Mass Destruction – WMD)
2. Zgodność zastosowania BMR z motywami, celami i logiką działania podmiotów pozapaństwowych
3. Broń nuklearna i radiologiczna – prawdopodobieństwo uzyskania i użycia przez podmioty pozapaństwowe
 - 3.1. Uzyskanie broni nuklearnej i radiologicznej – potencjalne źródła i metody; Broń nuklearna; Broń radiologiczna
 - 3.2. Aspekty operacyjne – transport, detonacja oraz konsekwencje użycia
4. Broń biologiczna i chemiczna – prawdopodobieństwo uzyskania i użycia przez podmioty pozapaństwowe
 - 4.1. Uzyskanie broni B i C – możliwości i ograniczenia; Samodzielna produkcja broni chemicznej; Samodzielna produkcja broni biologicznej

- 4.2. Aspekty operacyjne – transport, rozprzestrzenianie, skutki użycia broni B i C
5. Ocena zagrożenia państw transatlantyckich działaniami z użyciem BMR w świetle dotychczasowych doświadczeń

Rozdział VI. Zastosowanie przez podmioty pozapaństwowe technologii informatycznych (information technologies – IT) jako zagrożenie asymetryczne

1. Definicja problemu oraz określenie specyfiki działań z użyciem technologii informatycznych
 - 1.1. Pojęcie walki informacyjnej (information warfare – IW)
 - 1.2. Specyfika działań w cyberprzestrzeni – czynniki decydujące o atrakcyjności dla podmiotów pozapaństwowych
2. Podstawowe kategorie działań podmiotów pozapaństwowych w cyberprzestrzeni – IT jako broń (środek walki informatycznej) oraz narzędzie pomocnicze
 - 2.1. Wykorzystanie IT w celach pomocniczych i jako force multiplier
 - 2.2. IT jako broń – rodzaje i środki ataków
3. Zastosowanie IT przez poszczególne kategorie podmiotów pozapaństwowych – zakres i rodzaje wykorzystywanych metod oraz cele ich użycia
 - 3.1. Terrorystyci a działania z użyciem IT. Problem cyberterroryzmu
 - 3.2. Cyberprzestępczość (cybercrime) a kwestia wykorzystania IT przez transnarodowe grupy przestępcze
 - 3.3. Zagrożenia ze strony innych podmiotów działających w cyberprzestrzeni. Problem hakerstwa i hakywizmu
4. Ocena zagrożeń związanych z użyciem IT

Zakończenie

Bibliografia

Indeks