

Założenia działań w cyberprzestrzeni
Piotr T. Dela

Spis treści

Wstęp 1

1. Cyberprzestrzeń jako środowisko walki 9

1.1. Istota walki 10

1.2. Współczesny wymiar konfliktu zbrojnego i wojny 25

1.3. Cyberprzestrzeń jako domena operacyjna 34

2. Elementy bezpieczeństwa cyberprzestrzeni 51

2.1. Informacja i przestrzeń informacyjna 52

2.2. Systemy informacyjne i systemy krytyczne 65

2.3. Bezpieczeństwo informacji, informacyjne i teleinformatyczne 74

2.4. Wymagania stawiane przed systemami informacyjnymi i teleinformatycznymi 86

3. Charakterystyka zagrożeń bezpieczeństwa cyberprzestrzeni 95

3.1. Zagrożenia informacyjne 96

3.2. Zagrożenia informatyczne 110

3.3. Zagrożenia kinetyczne 121

3.4. Inwigilacja, szpiegostwo i rozpoznanie 126

4. Wyznaczniki działań w cyberprzestrzeni 135

4.1. Czynniki walki 138

4.2. Zasady i reguły walki 146

4.3. Siła, potęga i potencjał 158

5. Klasyfikacja działań w cyberprzestrzeni	163
5.1. Cele realizowane w cyberprzestrzeni	164
5.2. Poziomy działań	173
5.3. Elementy konfliktu w cyberprzestrzeni	179
5.4. Działania profilaktyczno-ochronne	185
5.5. Wykorzystanie cyberprzestrzeni w poglądach narodowych i NATO	194
5.6. Wykorzystanie cyberprzestrzeni według poglądów rosyjskich	201
6. System walki w cyberprzestrzeni	209
6.1. Charakterystyka systemu walki	210
6.2. Tworzenie systemu walki	215
6.3. Elementy systemu	219
Zakończenie	239
Bibliografia	241
Spis rysunków i tabel	255