

SPIS TREŚCI

WSTĘP	5
SUMMARY	11
ROZDZIAŁ I	
Polityka bezpieczeństwa cybernetycznego. Konceptualizacja pojęcia	13
1.1. Wybrane aspekty konceptualizacji polityki bezpieczeństwa cybernetycznego	17
1.2. Proces zmian w postrzeganiu pojęcia bezpieczeństwa cybernetycznego	21
1.3. Cyberbezpieczeństwo z perspektywy nauk o polityce	29
1.4. Podsumowanie	31
ROZDZIAŁ II	
Wybrane aspekty polityki cyberbezpieczeństwa w perspektywie państw Europy Środkowo-Wschodniej	35
2.1.1. Polityka cyberbezpieczeństwa jako wyzwanie dla inicjatywy gospodarczo-politycznej państw Trójmorza	37
2.1.2. Historia i współczesność	39
2.1.3. Cele i zadania Trójmorza	40
2.1.4. Trójmorze vs Unia Europejska?	42
2.1.5. Rola Stanów Zjednoczonych w polityce Trójmorza	43
2.1.6. Charakterystyka państw Trójmorza	45
2.1.7. Odmienne interesy państw Trójmorza	48
2.1.8. Wyzwania polityki cyberbezpieczeństwa dla Trójmorza	51
2.1.9. Wnioski	56
2.2. Strategie cyberbezpieczeństwa państw Grupy Wyszehradzkiej	57
2.2.1. Główne założenia badawcze	58
2.2.2. Grupa Wyszehradzka	59
2.2.3. Główne determinanty polityki bezpieczeństwa Grupy Wyszehradzkiej	61
2.2.4. Wybrane cyberincydenty w Europie Środkowo-Wschodniej	63
2.2.5. Strategie cyberbezpieczeństwa państw Grupy Wyszehradzkiej	66
2.2.6. Podsumowanie	74
2.3. Wnioski	77
ROZDZIAŁ III	
Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej	79
3.1. Cyberbezpieczeństwo	81
3.2. Polityczny wymiar cyberbezpieczeństwa	83
3.3. Dokument: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022	85
3.4. Cele cyberstrategii	88
3.5. Budowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa	88
3.6. Wnioski	97
ROZDZIAŁ IV	
Wybrane aspekty polityki cyberbezpieczeństwa w perspektywie lokalnej	99
4.1.1. Współpraca instytucji publicznych w zakresie cyberbezpieczeństwa wśród dzieci i młodzieży	102
4.1.2. Współpraca między instytucjami	103
4.1.3. Innowacja jako źródło sukcesu	105
4.1.4. Czynniki wpływające na możliwość niepowodzenia projektu	107
4.1.5. Projekt edukacja dla cyberbezpieczeństwa	109
4.1.6. Realizacja projektu	111
4.1.8. Podsumowanie	116
4.2. Cyberbezpieczeństwo wybranych podmiotów w regionie Pomorza Środkowego	117
4.2.1. Metodologia	119
4.2.2. Badanie	120
4.2.3. Podsumowanie	124
4.3. Wnioski	126

ROZDZIAŁ V

Szanse i zagrożenia dla życia publicznego w kontekście funkcjonowania cybertechnologii	131
5.1. Wybrane wady i zalety cyberprzestrzeni	134
5.2. Cyberspołeczeństwo	136
5.3. Ruchy społeczne	140
5.4. Cyberpornografia	143
5.5. Podsumowanie	147

ROZDZIAŁ VI

Stan wiedzy o cyberzagrożeniach w kontekście polityki bezpieczeństwa cybernetycznego państwa	149
6.1. Definicja cyberzagrożenia	151
6.2. Wybrane cyberzagrożenia	155
6.3. Globalny i prawny wymiar cyberprzestrzeni	159
6.4. Anonimowość jako wyzwanie dla polityki bezpieczeństwa	160
6.5. Problem „jawności” cyberzagrożeń	161
6.6. Podsumowanie	163

ROZDZIAŁ VII

Cyberzagrożenia jako wyzwania polityczne. Problemy i perspektywy	165
7.1.1. Zjawisko cyberterroryzmu i jego znaczenie w perspektywie polityki bezpieczeństwa	169
7.1.2. Cyberprzestrzeń	170
7.1.3. Terroryzm tradycyjny a cyberterroryzm	171
7.1.4. Definicje cyberterroryzmu	173
7.1.5. Wybrane aspekty cyberterroryzmu	175
7.1.6. Pojęcie cyberterroryzmu wobec innych cyberzagrożeń	177
7.1.6.1. Cyberprzestępstwa	177
7.1.6.2. Hakerzy	178
7.1.6.3. Cyberatak	180
7.1.6.4. Phishing	183
7.1.6.5. Cyberwywiad	185
7.1.6.6. Cyberpropaganda	186
7.1.7. Wolność vs bezpieczeństwo	188
7.1.8. Podsumowanie	188
7.2.1. Cyberwojna – jako element współczesnego konfliktu politycznego i militarnego	189
7.2.2. Innowacyjne technologie a cyberwojna	190
7.2.3. Konwencjonalne działania a cyberwojna	194
7.2.4. Wątpliwości definicyjne	198
7.2.5. Współczesny charakter cyberwojny	200
7.2.6. Wnioski	202
ZAKOŃCZENIE	205
BIBLIOGRAFIA	211