

Spis treści

Wstęp	7
Rozdział 1. Pojęcia cyberprzestrzeni, cyberprzestępstw i cyberterroryzmu – próba reasumpcji	11
1.1. Cyberprzestrzeń.....	11
1.2. Bezpieczeństwo w cyberprzestrzeni.....	14
1.3. Walka informacyjna w cyberprzestrzeni.....	19
1.4. Cyberprzestępczość.....	21
1.5. Terroryzm.....	35
1.6. Cyberterroryzm.....	61
Rozdział 2. Polityki ochrony cyberprzestrzeni w Unii Europejskiej	73
2.1. Zapobieganie terroryzmowi jako element procesu integracji europejskiej w latach 1951-1999	73
2.2. Unia Europejska a zwalczanie terroryzmu i cyberterroryzmu w latach 2001-2015.....	84
Rozdział 3. Polityka ochrony cyberprzestrzeni w Stanach Zjednoczonych Ameryki	118
3.1. Cyberprzestrzeń USA jako teatr działań wojennych	118
3.2. Ramowe doktryny obrony cybernetycznej USA....	121

4	3.3. Ramowe założenia Ochrony Infrastruktury Krytycznej w USA.....	125
	3.4. Dokumenty strategiczne dotyczące krajowego i międzynarodowego bezpieczeństwa cyberprzestrzeni opracowane przez USA.....	132
	Rozdział 4. Polityki i strategie ochrony cyberprzestrzeni w Rzeczypospolitej Polskiej	151
	4.1. Strategie Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej przyjęte w latach 1990- 2017.....	151
	4.2. Polityki i programy ochrony cyberprzestrzeni Rzeczypospolitej Polskiej.....	169
	Rozdział 5. Strategiczne założenia ochrony infrastruktury krytycznej Rzeczypospolitej Polskiej	195
	5.1. Definicja infrastruktury krytycznej w Polsce i Unii Europejskiej.....	195
	5.2. Podstawy prawne ochrony infrastruktury krytycznej w Polsce	199
	5.3. Instytucje powołane do ochrony infrastruktury krytycznej	221
	Rozdział 6. Infrastruktura krytyczna Rzeczypospolitej Polskiej	236
	6.1. Infrastruktura krytyczna RP – systematyka.....	236
	6.2. System łączności	258
	6.3. System finansowy	267
	6.4. System zaopatrzenia w żywność.....	271
	6.5. System zaopatrzenia w wodę	290
	6.6. System ochrony zdrowia.....	291
	6.7. System transportowy.....	294

6.8. System ratowniczy	295	I 5
6.9. System zapewniający ciągłość działania administracji publicznej	298	
6.10. System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	303	
6.11. Infrastruktura a zagrożenie cyberterroryzmem – podsumowanie.....	306	
Rozdział 7. Problemy ochrony infrastruktury krytycznej RP przed zagrożeniami cyberterrorystycznymi	321	
7.1. Problemy definicyjne pojęcia infrastruktury krytycznej	321	
7.2. Definicja infrastruktury krytycznej jako czynnik warunkujący skuteczność jej identyfikacji i ochrony	329	
7.3. Metodologia rozwiązań regulacyjnych a zapewnienie cyberbezpieczeństwa systemów infrastruktury krytycznej w Polsce	345	
7.4. Niejasności dotyczące odpowiedzialności prawnej za bezpieczeństwo infrastruktury krytycznej	351	
7.5. Sektor elektroenergetyczny infrastruktury krytycznej jako szczególnie narażony na atak cyberterrorystyczny.....	364	
Podsumowanie.....	376	
Bibliografia.....	384	
Spis tabel, map, rysunków i wykresów.....	393	