

# Spis treści

Wstęp.....	7
<b>Rozdział 1. Pojęcia cyberprzestrzeni, cyberprzestępstw i cyberterroryzmu – próba reasumpcji.....</b>	<b>11</b>
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
<b>Rozdział 2. Polityki ochrony cyberprzestrzeni w Unii Europejskiej.....</b>	<b>73</b>
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
<b>Rozdział 3. Polityka ochrony cyberprzestrzeni w Stanach Zjednoczonych Ameryki.....</b>	<b>118</b>
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
	<b>Rozdział 4. Polityki i strategie ochrony cyberprzestrzeni w Rzeczypospolitej Polskiej .....</b>	<b>151</b>
	4.1. Strategie Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej przyjęte w latach 1990- 2017.....	151
	4.2. Polityki i programy ochrony cyberprzestrzeni Rzeczypospolitej Polskiej.....	169
	<b>Rozdział 5. Strategiczne założenia ochrony infrastruktury krytycznej Rzeczypospolitej Polskiej .....</b>	<b>195</b>
	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
	<b>Rozdział 6. Infrastruktura krytyczna Rzeczypospolitej Polskiej .....</b>	<b>236</b>
	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	1 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	
<b>Rozdział 7. Problemy ochrony infrastruktury krytycznej RP przed zagrożeniami cyberterrorystycznymi .....</b>	<b>321</b>	
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	
<b>Podsumowanie.....</b>	<b>376</b>	
<b>Bibliografia.....</b>	<b>384</b>	
<b>Spis tabel, map, rysunków i wykresów.....</b>	<b>393</b>	