

SPIS TREŚCI

Wykaz skrótów	VII
Wstęp	1
1 Geneza i istota bezpieczeństwa informacyjnego	11
1.1 Geneza bezpieczeństwa informacyjnego w Unii Europejskiej	12
1.2 Istota bezpieczeństwa informacyjnego w Unii Europejskiej	23
2 Strategia cyberbezpieczeństwa Unii Europejskiej w XXI w.	35
2.1 Paradygmat bezpieczeństwa państwa w stosunkach międzynarodowych	36
2.2 Europejska strategia bezpieczeństwa jako instrument polityki cyberbezpieczeństwa Unii Europejskiej	45
2.3 Istota strategii ochrony cyberprzestrzeni Unii Europejskiej	60
3 Uwarunkowania cyberbezpieczeństwa Unii Europejskiej	77
3.1 Istota i zakres cyberterroryzmu jako zagrożenia w XXI w.	80
3.2 Uwarunkowania zagrożeń cyberterrorystycznych w Unii Europejskiej	93
3.2.1. Uwarunkowania zewnętrzne	93
3.2.2. Uwarunkowania wewnętrzne	108
4 Prawne standardy cyberbezpieczeństwa Unii Europejskiej	121
4.1 Międzynarodowe normy prawne w zakresie zwalczania cyberterroryzmu	122
4.1.1. Rada Europy wobec cyberprzestępczości	122
4.1.2. Interpol w walce z cyberterroryzmem	128
4.1.3. Organizacja Narodów Zjednoczonych w walce z cyberterroryzmem	131
4.2 Prawo unijne wobec cyberterroryzmu	134
4.2.1. Prawo pierwotne Unii Europejskiej wobec cyberterroryzmu	134
4.2.1.1. Traktat z Maastricht	135
4.2.1.2. Traktat z Amsterdamu	138
4.2.1.3. Traktat z Nicei	143
4.2.1.4. Traktat z Lizbony	146
4.2.2. Prawo wtórne Unii Europejskiej wobec cyberterroryzmu	155
4.2.3. Instytucjonalny wymiar zwalczania cyberprzestępczości w prawie Unii Europejskiej	172

5	Realizacja polityki cyberbezpieczeństwa Unii Europejskiej	181
5.1	Unia jako podmiot polityki ochrony cyberbezpieczeństwa	182
5.2	Instrumenty polityki cyberbezpieczeństwa	199
5.2.1.	Europol i SIS	199
5.2.2.	Eurojust	203
5.2.3.	Agencja UE ds. Cyberbezpieczeństwa (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji)	205
5.2.4.	Europejskie Centrum ds. Walki z Cyberprzestępczością	207
5.2.5.	Decyzje ramowe i strategie UE dotyczące problematyki zwalczania cyberterroryzmu	208
6	Implementacja polityki cyberbezpieczeństwa w Unii Europejskiej na przykładzie wybranych państw	225
6.1	Implementacja polityki cyberbezpieczeństwa w Estonii	226
6.1.1.	Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa	226
6.1.2.	Instytucjonalny wymiar polityki cyberbezpieczeństwa	230
6.2	Implementacja polityki cyberbezpieczeństwa w Polsce	233
6.2.1.	Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa	233
6.2.2.	Polski Kodeks karny wobec polityki cyberbezpieczeństwa	245
6.2.3.	Wymiar instytucjonalny zwalczania cyberterroryzmu w Polsce	259
6.2.4.	Dyrektywa NIS w prawie polskim	269
6.3	Implementacja polityki cyberbezpieczeństwa w RFN	281
6.3.1.	Podstawa prawna polityki cyberbezpieczeństwa	281
6.3.2.	Instytucjonalny wymiar polityki cyberbezpieczeństwa RFN	295
6.4	Implementacja polityki cyberbezpieczeństwa we Francji	300
6.4.1.	Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa	300
6.4.2.	Instytucjonalny wymiar polityki cyberbezpieczeństwa	312
6.5	Implementacja polityki cyberbezpieczeństwa w Wielkiej Brytanii	316
6.5.1.	Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa	316
6.5.2.	Instytucjonalny wymiar polityki cyberbezpieczeństwa	324
7	Skutki i perspektywy rozwoju strategii i polityki cyberbezpieczeństwa Unii Europejskiej	335
7.1	Skutki polityki i strategii cyberbezpieczeństwa Unii Europejskiej	336
7.2	Perspektywy polityki i strategii cyberbezpieczeństwa Unii Europejskiej	347
	Zakończenie	355
	Bibliografia	363