

Zjawisko cyberterroryzmu w Polsce, jako zagrożenie XXI wieku

Wstęp.....7

Rozdział I.

Zjawisko cyberterroryzmu i jego istota

1.1. Pojęcia związane ze zjawiskiem cyberterroryzmu9

1.1.1. Internet..... 9

1.1.2. Pojęcie cyberprzestępczości..... 10

1.1.3. Cyberprzestrzeń..... 13

1.2. Istota cyberterroryzmu14

Rozdział II.

Cyberterroryzm jako nowa odsłona terroryzmu

2.1. Zagrożenia związane z cyberterroryzmem..... 21

2.2. Podmioty dokonujące ataków cyberterrorystycznych..... 23

2.3. Przyczyny ataków cyberterrorystycznych26

2.4. Fazy i metody cyberataków27

2.4. Przykłady ataków cyberterrorystycznych32

2.5. Ochrona sprzętu komputerowego przed cyberatakami..... 35

2.6. Perspektywy rozwojowe cyberterroryzmu38

Rozdział III.

Prawne podstawy bezpieczeństwa informacyjnego Polski

3.1. Unia Europejska wobec zjawiska cyberterroryzmu41

3.1.1. Konwencja Rady Europy o cyberprzestępczości42

3.1.2. Decyzja Ramowa Rady Unii Europejskiej w sprawie ataków

na systemy informatyczne	44
3.1.3. Komunikat 'W kierunku ogólnej strategii zwalczania cyberprzestepczosci'	46
3.1.4 Strategia pracy i konkretnych środków służących zwalczaniu cyberprzestepczosci	48
3.2 Zwalczanie cyberterroryzmu w prawie polskim	49
3.2.1. Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej.....	49
3.2.2. Kodeks karny.....	51
3.2.3. Rządowy program w zakresie ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016.....	53
3.3 Państwowe instytucje nadzoru i ochrony uzytkownikow przed cyberprzestepczoscia.....	55
3.3.1. Rządowy Zespół Reagowania na Incydenty Komputerowe.....	55
3.3.2. CERT Polska	56
3.3.3. Prokuratura i sady powszechne.....	57
3.3.4. Policja.....	58
3.3.5. Inne organy właściwe związane z cyberprzestepczoscia	59
3.4 Polska w międzynarodowym systemie walki z cyberprzestepczoscia	60
3.4.1. NATO.....	60
3.4.2. IMPACT	62
3.4.3. ENISA	63
Podsumowanie	65
Bibliografia:	67
Streszczenie:	71