
Spis treści

Wprowadzenie	11
 Część I	
CYBERTERRORYZM – WYMIAR POLITYCZNY	19
1. Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku	21
Andrzej Podraza	
Wstęp	21
1.1. Transformacja porządku międzynarodowego po zakończeniu zimnej wojny	23
1.2. Pojęcie cyberterroryzmu	26
1.3. Ataki w cyberprzestrzeni	36
Zakończenie	40
Bibliografia	41
2. Państwo wobec cyberterroryzmu	44
Wojciech Gizicki	
Wstęp	44
2.1. Przestrzeń cybernetyczna	45
2.2. Zagrożenia cyberterrorystyczne	46
2.3. Przeciwdziałanie cyberterroryzmowi	49
Zakończenie	53
Bibliografia	54
3. The cyberwar challenge to NATO	56
Martin Libicki	
Introduction	56
3.1. What is cyberwar?	56

3.2. How should NATO react to cyberwar?	57
3.3. Protecting NATO's conventional warfighting capability	61
Conclusion	64
Bibliography	64
4. Strategia Stanów Zjednoczonych wobec problemu bezpieczeństwa cyberprzestrzeni	65
Łukasz Czebotar	
Wstęp	65
4.1. Geneza opracowania całościowej strategii bezpieczeństwa w cyberprzestrzeni	67
4.2. Rozwiązania przewidziane w Narodowej Strategii Bezpieczeństwa Cyberprzestrzeni (NSSC)	69
4.2.1. Poziomy najbardziej podatne na ataki	71
4.2.2. Kluczowe priorytety	72
4.2.2.1. Narodowy System Reagowania (NCSRS)	73
4.2.2.2. Narodowy Program Redukcji Zagrożeń i Wrażliwości (NCSTVRP)	76
4.2.2.3. Narodowy Program Ostrzegania i Szkolenia (NCSATP)	77
4.2.2.4. Bezpieczeństwo Cyberprzestrzeni Rządowej (SGC)	79
4.2.2.5. Bezpieczeństwo Państwowe i Współpraca Międzynarodowa w Kwestii Bezpieczeństwa Cyberprzestrzeni (NSICSC)	81
Zakończenie	82
Bibliografia	83
5. Cyberbezpieczeństwo infrastruktury krytycznej – priorytet strategii obrony USA?	85
Dominika Dziwisz	
Wstęp	85
5.1. Ochrona infrastruktury krytycznej USA – rozwiązania administracji Billa Clintona	86
5.2. Rozwiązania administracji George'a W. Busha	91
5.3. Rozwiązania administracji Baracka Obamy	94
Zakończenie	96
Bibliografia	97
6. Cyberdżihad. Wykorzystanie internetu przez współczesny terroryzm islamistyczny	99
Stanisław Kosmyńka	
Wstęp	99
6.1. Digitalizacja dżihadyzmu	101
6.2. Propaganda i wizerunek	105
6.3. Dostęp do informacji i (auto)rekrutacja	112
Bibliografia	122

Część II

CYBERTERRORYZM – WYMIAR PRAWNY I INSTYTUCJONALNY

125

1. Strategie zwalczania cyberterroryzmu – aspekty prawne	127
Mariusz Czyżak	
Wstęp	127
1.1. Pojęcie cyberterroryzmu	129
1.2. Prawny wymiar istniejących strategii związanych ze zwalczaniem cyberterroryzmu	130
1.3. Obowiązki przedsiębiorców telekomunikacyjnych a przeciwdziałanie cyberterroryzmowi	134
Zakończenie	138
Bibliografia	140
2. Rozwój technologii informacyjnych i komunikacyjnych oraz związanych z nimi zagrożeń – wybrane aspekty prawne	142
Paweł Fajgielski	
2.1. Rozwój technologii. Reagowanie na zagrożenia	142
2.2. Pojęcie „cyberterroryzm”	144
2.3. Regulacje prawne odnoszące się do cyberterroryzmu	146
2.4. Projektowane rozwiązania prawne odnoszące się do cyberterroryzmu	149
Zakończenie	150
Bibliografia	151
3. Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem	152
Aleksandra Suchorzewska	
Bibliografia	159
4. Bezpieczeństwo teleinformatyczne – wymiar instytucjonalny	161
Marek Grajek	
5. Wirtualna przestrzeń publiczna – szansa czy zagrożenie dla administracji?	170
Wojciech Wytrzątek	
Wstęp	170
5.1. Sfera publiczna	171
5.2. Sfera zadań publicznych	173
5.3. Przestrzeń publiczna	175

5.4. Cyberprzestrzeń	179
5.5. Wirtualna przestrzeń publiczna	182
Zakończenie	184
Akty prawne	185
Bibliografia	186
6. Prawa człowieka a wprowadzenie stanów nadzwyczajnych z uwagi na działania w cyberprzestrzeni	189
Michał Skwarzyński	
Wstęp	189
6.1. Stany nadzwyczajne a prawa jednostki	191
6.2. Międzynarodowe gwarancje praw człowieka w czasie stanu nadzwyczajnego	193
6.2.1. Stanowisko Europejskiego Trybunału Praw Człowieka wobec praktyki wprowadzania stanów nadzwyczajnych	196
6.3. Rodzaje stanów nadzwyczajnych w Polsce	197
6.3.1. Ograniczenia praw i wolności człowieka z uwagi na wprowadzenie stanów nadzwyczajnych	199
6.3.2. Wprowadzenie stanów nadzwyczajnych z uwagi na działania w cyberprzestrzeni	202
6.3.3. Problem zakresu ingerencji w prawa i wolności człowieka w czasie stanu nadzwyczajnego wprowadzonego z uwagi na działania w cyberprzestrzeni	204
Zakończenie	205
Bibliografia	205
7. Internetowy wigilantyzm – zagrożenie czy szansa dla społeczeństwa globalnego?	208
Małgorzata Dziewanowska	
Wstęp	208
7.1. Podstawowe zagadnienia	210
7.2. Popularne typy internetowego wigilantyzmu	212
7.2.1. Ośmieszanie	212
7.2.2. Prześladowanie (<i>cyberbullying</i>)	213
7.2.3. Identyfikowanie sprawców przestępstw	214
7.2.4. Społeczna sprawiedliwość	215
7.2.5. Przeciwdziałanie terroryzmowi	216
7.2.6. Działalność przeciwko pedofilii	217
7.3. Metody perswazji	217
7.4. Anonimowość i cybertożsamość	219
7.5. Zagadnienia prawne	220
Zakończenie	221
Bibliografia	222

8. Czy haker może wypowiedzieć wojnę? Kазus Wikileaks	224
Paweł Potakowski	
Wstęp	224
8.1. Pojęcia podstawowe	226
8.2. Haker aktywista	227
8.3. Haker przestępca	229
8.4. Haker terrorysta	231
8.5. Problemowi Anonimowi	233
8.6. Kазus Wikileaks	234
Zakończenie	236
Bibliografia	238

Część III

CYBERTERRORYZM – WYMIAR PRAWNOKARNY	241
--	-----

1. Prawnokarne środki przeciwdziałania cyberterroryzmowi	243
Krzysztof Wiak	
Bibliografia	256
2. Przestępstwa przeciwko integralności i dostępności do zapisu danych informatycznych jako przestępstwa o charakterze terrorystycznym	258
Zuzanna Barbara Gądzik	
Bibliografia	274
3. Odpowiedzialność karna za przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni	277
Stanisław Dziwisz	
Wstęp	277
3.1. Cyberprzestrzeń	278
3.2. Cyberterroryzm	279
3.3. Terroryzm a przestępstwo o charakterze terrorystycznym	281
3.4. Przepisy regulujące odpowiedzialność za cyberterroryzm w polskim prawie karnym	283
3.5. Kwalifikacja najpoważniejszych zachowań terrorystycznych popełnionych w cyberprzestrzeni	285
3.5.1. Sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w wielkich rozmiarach	286